

Key Capacity for Product Sources with Application to Stationary Gaussian Processes

Jingbo Liu Paul Cuff Sergio Verdú

Dept. of Electrical Eng., Princeton University, NJ 08544

{jingbo,cuff,verdu}@princeton.edu

Abstract—We show that for product sources, rate splitting is optimal for secret key agreement using limited one-way communication between two terminals. This yields an alternative information-theoretic-converse-style proof of the tensorization property of a strong data processing inequality originally studied by Erkip and Cover and amended recently by Anantharam et al. We derive a water-filling solution of the communication-rate–key-rate tradeoff for a wide class of discrete memoryless vector Gaussian sources which subsumes the case without an eavesdropper. Moreover, we derive an explicit formula for the maximum secret key per bit of communication for all discrete memoryless vector Gaussian sources using a tensorization property and a variation on the enhanced channel technique of Weingarten et al. Finally, a one-shot information spectrum achievability bound for key generation is proved from which we characterize the communication-rate–key-rate tradeoff for stationary Gaussian processes.

Index Terms—Random number generation, source coding, Gaussian processes, Correlation coefficient, Decorrelation, Fourier transforms, MIMO.

I. INTRODUCTION

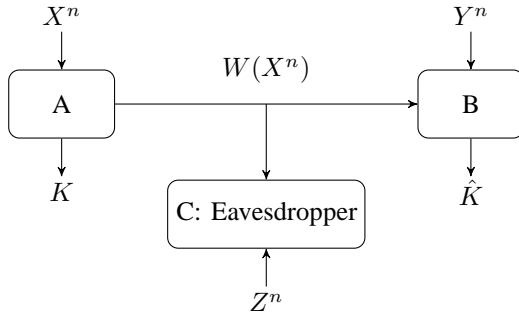


Figure 1. The basic model for secret key agreement between two terminals A and B allowing public communication from A to B.

An important scenario for secret key agreement (a.k.a. key generation) arises when terminals at distant locations have access to correlated sources and are allowed to communicate publicly in order to decide on a key which is kept unknown to an eavesdropper.

This paper was presented in part at 2014 IEEE International Symposium on Information Theory (ISIT). Copyright (c) 2014 IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending a request to pubpermissions@ieee.org.

The fundamental limit on the amount of secret key that can be generated from discrete memoryless sources was studied in [1],[2], where single-letter solutions were derived for the class of protocols allowing limited one-way communication from one terminal to the other. However, for many models of interest in practice, the key capacity remains unknown, since the optimizations over auxiliary random variables in those single-letter formulas are usually hard to solve.

In [3] the fundamental limit was extended to sources with continuous alphabets; and it was shown that for vector Gaussian sources, which are natural models of multiple input multiple output (MIMO) systems, one auxiliary random variable suffices to characterize the rate region, instead of two in the general case [1], and it is enough to consider auxiliary random vectors that are jointly Gaussian with the sources. This observation is formally stated in Fact 1 ahead, the proof of which in [3] was based on the enhancement technique introduced by Weingarten et al. [4]. Consequently, the capacity region for vector Gaussian sources was posed as a (generally non-convex) matrix optimization problem. Still, an explicit formula for the key capacity was not derived except for scalar Gaussian sources.

In this paper we provide an explicit formula for the key capacity of vector Gaussian sources by considering a more general setup: the key capacity of arbitrary product sources. Specifically, suppose terminals A and B and an eavesdropper observe discrete memoryless vector sources $\mathbf{X} = (X_i)_{i=1}^L$, $\mathbf{Y} = (Y_i)_{i=1}^L$ and $\mathbf{Z} = (Z_i)_{i=1}^L$ respectively, where

$$P_{\mathbf{X}\mathbf{Y}} = \prod_{i=1}^L P_{X_i Y_i}, \quad (1)$$

$$P_{\mathbf{X}\mathbf{Z}} = \prod_{i=1}^L P_{X_i Z_i}. \quad (2)$$

We call $(\mathbf{X}, \mathbf{Y}, \mathbf{Z})$ a *product source* because of the structure of its joint probability distribution. An example of product sources is illustrated in Figure 2.¹ The maximal rate of secret key achievable as a function of public communication rate r from A to B is denoted as $R(r)$. We show that

$$R(r) = \max_{\sum_{i=1}^L r_i \leq r} \sum_{i=1}^L R_i(r_i), \quad (3)$$

¹Actually Figure 2 only illustrates an unnecessarily special case of (1) and (2) where $P_{\mathbf{X}\mathbf{Y}\mathbf{Z}} = \prod_{i=1}^L P_{X_i Y_i Z_i}$; c.f. Section II-B.

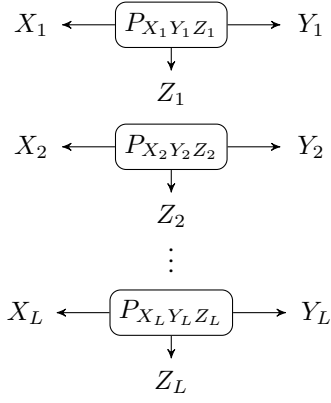


Figure 2. An illustration of the product sources in (1) and (2).

where $R_i(r_i)$ is the key-communication function corresponding to the i -th source triple: (X_i, Y_i, Z_i) . This is analogous to a result due to Shannon [5] on the rate distortion function of a product source with a separable distortion measure, which is obtained by summing the rates and distortions of points in the individual rate-distortion curves with the same slope.

In the case of jointly vector Gaussian sources without an eavesdropper (or with an eavesdropper but under a certain commutative condition on the covariance matrices), one can always apply separate invertible linear transforms on the vectors observed at A and B so that the source distribution is of the form in (1) and (2), thus deriving an explicit formula of $R(r)$ utilizing corresponding results of scalar Gaussian sources. The solution displays a “water filling” behavior similar to the rate distortion function of vector Gaussian sources (e.g. [6]).

When the eavesdropper is present, the key-communication function is not always explicitly derived for vector Gaussian sources since the aforementioned commutative condition does not always hold. This motivates us to consider the maximum amount of secret key obtainable per bit of communication, denoted by $\eta_Z(X; Y)$. For vector Gaussian sources $\eta_Z(\mathbf{X}; \mathbf{Y})$ can always be explicitly found; and in order to upper bound $\eta_Z(\mathbf{X}; \mathbf{Y})$ we use an idea similar to but different than the *enhanced channel* introduced in [4]. Analogous to $\eta_Z(X; Y)$ is the notion of channel capacity per unit cost, introduced in [7]. As in the case of channel capacity per unit cost [7], a general formula for $\eta_Z(X; Y)$ can be obtained which is usually easier to compute both numerically and analytically. Some other general properties of $\eta_Z(X; Y)$ are discussed, including a formula of this quantity for product sources.

There is a curious connection between our results for product sources and the tensorization property of a strong data processing inequality originally studied by Erkip and Cover [8] and amended recently by Anantharam et al. [9]. Suppose $P_{XY} = P_X P_{Y|X}$ is given, and

$$s^*(X; Y) = \sup_{U \sim X \rightarrow Y, I(U; X) \neq 0} \frac{I(U; Y)}{I(U; X)}. \quad (4)$$

In [8] it was mistakenly claimed that

$$s^*(X; Y) = \rho_m^2(X; Y) \quad (5)$$

where $\rho_m^2(X; Y)$ denotes the maximal correlation coefficient [10]. In fact, [9] shows that (5) does not hold in general and gives a general but less explicit expression:

$$s^*(X; Y) = \sup_{Q_X \neq P_X} \frac{D(Q_Y \| P_Y)}{D(Q_X \| P_X)} \quad (6)$$

where $Q_X \rightarrow P_{Y|X} \rightarrow Q_Y$. Although $\rho_m^2(X; Y)$ and $s^*(X; Y)$ tensorize and do agree for some simple distributions of P_{XY} such as Gaussian and binary with equiprobable marginals, it was already shown in [11] that they are not equal in general. Moreover, they are both closely linked to the problem of key generation [10][12].³ To add one more connection between $s^*(X; Y)$ and key generation, we demonstrate that (3) implies the tensorization property of $s^*(X; Y)$.⁴ The tensorization property of $s^*(X; Y)$ turns out to be the key to many of its applications, c.f. [11] [15] [16]. In particular, it was shown in [11] via the tensorization of hypercontractivity of Markov operators.

Related to (memoryless) product Gaussian sources are (scalar) stationary Gaussian processes which generally have memory, since intuitively one can consider the spectral representation of stationary Gaussian processes and apply the insights from the above results concerning product sources. However there are several technical difficulties in turning this intuition into a formal proof; for example the known achievability bounds for the model under our consideration are mostly confined to memoryless sources. Thus as the first step of our proof we derive an original one-shot achievability bound via resolvability for general sources. It is relatively well known that resolvability can be applied to wiretap channels (see [17] and the references therein), and wiretap channel codes can be employed in the encoding schemes in key agreement (an idea due to [18]; see also [19, Section 22.4.3]). Based on these connections, a recent paper [20] derived upper and lower bounds on the key capacity for sources with memory. However those bounds may be loose, and they are still asymptotic (expressed in terms of probabilistic limsup of random variables) rather than one-shot. Moreover the setting therein is a special case of ours where the public communication rate is unlimited, and the proof technique involving modulo sums only applies to discrete sources, therefore those results are still not quite useful for resolving the achievable region for stationary Gaussian sources. In contrast, our achievability bound overcomes those issues by employing a different encoding scheme called *likelihood encoder* proposed recently in [21]. We then apply certain asymptotic approximation theorems for Toeplitz matrices when specializing to Gaussian processes.

Organization. The formal definition of the key generation problem with limited one-way communication, as well as the setup of product sources and stationary Gaussian sources, are presented in Section II. The main results are given in

²This notation defines a measure Q_Y via $Q_Y(A) := \int P_{Y|X=x}(A) dQ_X(x)$ for any measurable $A \subseteq \mathcal{Y}$.

³For the reason we just discussed, the $\rho_m^2(X; Y)$ in the expressions of efficiency functions in [12] should be replaced by $s^*(X; Y)$.

⁴Following our ISIT presentation of this work [13], Beigi and Gohari [14] extended such an idea and introduced several new tensorizing measures of correlation from the operational perspectives of coding theorems.

Section III. Section III-A gives the central result concerning key generation from general product sources and it analyzes the special case of product Gaussian sources culminating in the “water-filling” solution. The necessary and sufficient condition under which general vector Gaussian sources can be converted to product Gaussian sources is also identified. Section III-B begins with several general properties on the maximal secret key per bit of communication, and ends with a formula for this quantity for general vector Gaussian sources which may not be convertible to product sources. Section III-C presents the water-filling solution for the key-communication tradeoff for stationary Gaussian processes (Theorem 6) and discusses the intuition behind it. To prove Theorem 6, we derive a general one-shot achievability bound for key generation from sources with memory in Section IV, and then apply it in Section V to finish the achievability proof of Theorem 6. In Section VI we mention some related problems involving product sources/channels.

II. PRELIMINARIES

A. Key Generation with One-Way Communication: Basic Setup

Throughout this paper, random variables (but not excluding deterministic constants) are denoted by upper-case letters, and vectors and matrices are denoted in bold face.

Consider the source model illustrated in Figure 1. Stationary sources of blocklength n have the joint distribution $P_{X^n Y^n Z^n}$, where X_i^j is a short hand notation for $(X_i, \dots, X_j)^\top$ and $X^n := X_1^n$. Upon receiving X^n , terminal A computes an integer $K \in \mathcal{K}$ and a message $W \in \mathcal{W}$, possibly stochastically⁵, according to $P_{KW|X^n}$. The message W is then sent through a noiseless public channel to terminal B, and B computes the key $\hat{K} = \hat{K}(W(X^n), Y^n) \in \mathcal{K}$ based on its available information. The probability of error and the measure of security are defined by

$$\epsilon_n = \mathbb{P}[K \neq \hat{K}], \quad (7)$$

$$\nu_n = \log |\mathcal{K}| - H(K|W, Z^n). \quad (8)$$

A rate pair (R, r) is said to be achievable if a sequence of schemes can be designed to satisfy the following conditions on the probability of disagreement and security:

$$\limsup_{n \rightarrow \infty} \frac{1}{n} \log |\mathcal{W}| \leq r, \quad (9)$$

$$\liminf_{n \rightarrow \infty} \frac{1}{n} \log |\mathcal{K}| \geq R, \quad (10)$$

$$\lim_{n \rightarrow \infty} \epsilon_n = 0, \quad (11)$$

$$\lim_{n \rightarrow \infty} \nu_n = 0. \quad (12)$$

In the remainder of Section II-A we focus on the case of stationary memoryless sources with per-symbol distribution P_{XYZ} . The achievable rate region is defined as

$$\mathcal{R}(X, Y, Z) := \{(R, r) : (R, r) \text{ is achievable}\}, \quad (13)$$

⁵Here we allow stochastic encoders to be consistent with the achievability scheme in Section IV, although in the literature K and W have often been defined as functions of X^n .

and the key-communication function

$$R(r) := \sup\{R : (R, r) \in \mathcal{R}(X, Y, Z)\} \quad (14)$$

characterizes the maximal possible key rate given a certain public communication rate.

From [1], the region $\mathcal{R}(X, Y, Z)$ is the union of

$$[0, I(V; Y|U) - I(V; Z|U)] \times [I(U, V; X) - I(U, V; Y), \infty) \quad (15)$$

over all U, V such that $(U, V) - X - (Y, Z)$.

For key generation with one-way communication under our consideration, only P_{XY} and P_{XZ} affect the achievable key-communication rates. Although beyond those joint distributions we do not need further information about the source, it is customary to say that P_{XYZ} is stochastically degraded [6] if $X - Y - Z$ form a Markov chain under a joint distribution whose pairwise distributions are P_{XY} and P_{XZ} . In this case, the above region can be simplified to the union of

$$[0, I(V; Y) - I(V; Z)] \times [I(V; X) - I(V; Y), \infty) \quad (16)$$

over all V such that $V - X - (Y, Z)$.

For jointly Gaussian vectors $(\mathbf{X}, \mathbf{Y}, \mathbf{Z})$ it is generally not true that $P_{\mathbf{X}\mathbf{Y}\mathbf{Z}}$ is stochastically degraded. Thus it might seem remarkable that still only one auxiliary random variable is needed; and it can be chosen to be jointly Gaussian with the source vectors, as summarized below:

Fact 1 ([3]). Suppose X^L, Y^L , and Z^L are jointly Gaussian vectors of length L , and U and V are random variables such that $(U, V) - X^L - (Y^L, Z^L)$ form a Markov chain. Then there exists a random vector \bar{U}^L in \mathbb{R}^L such that \bar{U}^L, X^L are jointly Gaussian, $\bar{U}^L - X^L - (Y^L, Z^L)$, and

$$I(\bar{U}^L; X^L) - I(\bar{U}^L; Y^L) \leq I(U, V; X^L) - I(U, V; Y^L), \quad (17)$$

$$I(\bar{U}^L; Y^L) - I(\bar{U}^L; Z^L) \geq I(V; Y^L|U) - I(V; Z^L|U). \quad (18)$$

As a consequence of Fact 1 the region $\mathcal{R}(\mathbf{X}, \mathbf{Y}, \mathbf{Z})$ is the union of

$$[0, I(\mathbf{U}; \mathbf{Y}) - I(\mathbf{U}; \mathbf{Z})] \times [I(\mathbf{U}; \mathbf{X}) - I(\mathbf{U}; \mathbf{Y}), \infty) \quad (19)$$

over all \mathbf{U} such that $\mathbf{U} - \mathbf{X} - (\mathbf{Y}, \mathbf{Z})$ and \mathbf{U}, \mathbf{X} are jointly Gaussian. Note that $(\mathbf{U}, \mathbf{X}, \mathbf{Y}, \mathbf{Z})$ are necessarily jointly Gaussian as well because of the Markov chain condition.

B. Key Generation from Product Sources

A product source is just a particular stationary memoryless source in which $P_{\mathbf{X}\mathbf{Y}\mathbf{Z}}$ has the structure of (1) and (2). Hence the setup for a product source model is the same as the stationary case of Part II-A with the exception that X, Y and Z are replaced with L -vectors \mathbf{X}, \mathbf{Y} and \mathbf{Z} .

We remind the reader that $\mathcal{R}(X, Y, Z)$ in II-A depends only on P_{XY} and P_{XZ} , hence we do not need to define a product source with the more stringent condition of $P_{\mathbf{X}\mathbf{Y}\mathbf{Z}} = \prod_{i=1}^L P_{X_i Y_i Z_i}$.

III. MAIN RESULTS

A. Secret Key Generation from Product Sources

Suppose we know the function $R_i(r)$ for each “factor” in the product source; what can we say about $R(r)$ for the whole source? As Theorem 3 elucidates, the rate splitting approach in which we produce keys separately for each factor source (with appropriately selected rates) achieves the optimal key rate. This is analogous to a result in rate distortion theory [5] as remarked in the introduction.

Theorem 1. *In the problem of key generation from product sources satisfying (1) and (2), the maximum key rate satisfies*

$$R(r) = \max_{\sum_{i=1}^L r_i \leq r} \sum_{i=1}^L R_i(r_i), \quad (20)$$

where $R_i(r_i)$ is the key-communication function corresponding to the i 'th source triple (X_i, Y_i, Z_i) . Further, if $R_i(\cdot)$ is differentiable and (r_1^*, \dots, r_L^*) achieves the maximum in (20), then for each i , either $R_i(r_i^*) = \mu$ for some constant μ or $r_i^* = 0$.

Remark 1. The result of (20) can be equivalently expressed as $\mathcal{R}(\mathbf{X}, \mathbf{Y}, \mathbf{Z}) = \sum_{i=1}^L \mathcal{R}(X_i, Y_i, Z_i)$, where the summation is the Minkowski sum of sets in the Euclidean space.

Proof: Each key rate of $R_i(r_i^*)$ can be approached by a scheme that operates on the i 'th source triple separately using a communication rate of r_i^* . From (2), the combination of these schemes forms a legitimate scheme for the product source, since the keys generated by those schemes are independent and their combination is (asymptotically) independent of W and \mathbf{Z}^n . Thus \geq holds in (20) ⁶.

By (16) the achievable region $\mathcal{R}(X^L, Y^L, Z^L)$ is the union of

$$\begin{aligned} & [0, I(V; Y^L | U) - I(V; Z^L | U)] \\ & \times [I(U, V; X^L) - I(U, V; Y^L), \infty) \end{aligned} \quad (21)$$

over all (U, V) such that $(U, V) - X^L - (Y^L, Z^L)$. The achievable region with rate splitting is the union of

$$\begin{aligned} & \left[0, \sum_{i=1}^L I(V_i; Y_i | U_i) - \sum_{i=1}^L I(V_i; Z_i | U_i) \right] \\ & \times \left[\sum_{i=1}^L I(U_i, V_i; X_i) - \sum_{i=1}^L I(U_i, V_i; Y_i), \infty \right) \end{aligned} \quad (22)$$

over all (U_i, V_i) such that $(U_i, V_i) - X_i - (Y_i, Z_i)$, which contains the union of (21), according to Lemma 6 in Appendix A. Hence we also have \leq in (20).

The last claim in the theorem for differentiable $R_i(\cdot)$ can be verified from the KKT condition and the fact that $R_i(\cdot)$ is a concave function for each i . ■

From Theorem 3 we derive the communication-rate-key-rate tradeoff for product Gaussian sources. The solution displays a “water-filling” behaviour which is reminiscent of the rate-distortion function for Gaussian vectors [6].

⁶From this argument we see that \geq in (20) only requires (2) but not (1). In words, a rate-splitting key agreement scheme designed for product sources will be reliable and secure even if the \mathbf{Y} vector is correlated. This can only correlate the decoding errors, which are negligible anyway.

Theorem 2. *If (X^L, Y^L, Z^L) are product Gaussian sources, then the achievable communication and key rates are parameterized by $\mu > 0$ as*

$$r = \frac{1}{2} \sum_{i: \beta_i > \mu} \log \frac{\beta_i(\mu + 1)}{(\beta_i + 1)\mu}, \quad (23)$$

$$R = \frac{1}{2} \sum_{i: \beta_i > \mu} \log \frac{\beta_i + 1}{\mu + 1}, \quad (24)$$

where

$$\beta_i := \frac{\rho_{X_i Y_i}^2 - \rho_{X_i Z_i}^2}{1 - \rho_{X_i Y_i}^2}. \quad (25)$$

Remark 2. The usefulness of the i -th component of the product source is completely captured by β_i . In (23) and (24) the i 'th term enters the summations if and only if β_i is large enough; in other words, only the components that are strong enough are “on”. This is similar to water-filling over Gaussian channels (avoiding low SNR channels) and rate-distortion (neglecting to compress weak source components).

Remark 3. In Theorem 2 if we drop assumption that Y^L is Gaussian, i.e., only assume that (X^L, Y^L, Z^L) is a product source where X^L, Z^L are jointly Gaussian, then Theorem 2 will provide an inner bound on the achievable region. To see this, let Y_G^L be a random variable such that X^L and Y_G^L are jointly Gaussian, and (X^L, Y_G^L) has the same first and second order statistics as (X^L, Y^L) . If U is a Gaussian auxiliary random variable as in (19), then (U, Y_G^L) has the same first and second order statistics as (U, Y^L) . For arbitrary $P \ll Q$, define the *relative information*

$$i_{P||Q}(x) = \log \frac{dP}{dQ}(x) \quad (26)$$

as the logarithm of the Radon-Nikodym derivative. Then we have

$$\begin{aligned} & I(U; Y^L) - I(U; Y_G^L) \\ & = D(P_{UY^L} || P_U \times P_{Y^L}) - \mathbb{E} \left[i_{P_{UY_G^L} || P_U \times P_{Y_G^L}}(U, Y_G^L) \right] \end{aligned} \quad (27)$$

$$= D(P_{UY^L} || P_U \times P_{Y^L}) - \mathbb{E} \left[i_{P_{UY_G^L} || P_U \times P_{Y_G^L}}(U, Y^L) \right] \quad (28)$$

$$= D(P_{UY^L} || P_{UY_G^L}) - D(P_{Y^L} || P_{Y_G^L}) \quad (29)$$

$$\geq 0 \quad (30)$$

where (28) is because $i_{P_{UY_G^L} || P_U \times P_{Y_G^L}}(u, y^L)$ is only a second order polynomial of (u, y^L) . Hence the secret key can be generated more efficiently than in the Gaussian case:

$$I(U; X^L) - I(U; Y^L) \leq I(U; X^L) - I(U; Y_G^L) \quad (31)$$

$$I(U; Y^L) - I(U; Z^L) \geq I(U; Y_G^L) - I(U; Z^L). \quad (32)$$

For a positive-semidefinite matrix Σ , let $\Sigma^{-1/2}$ be a positive definite matrix such that $\Sigma^{-1/2} \Sigma \Sigma^{-1/2} = \mathbf{I}_r$, where \mathbf{I}_r denotes the identity matrix of dimension $r = \text{rank}(\Sigma)$. Also write $\Sigma^{-1} = (\Sigma^{-1/2})^2$, which is the matrix inverse when Σ is invertible. Note that under this definition $\Sigma^{-1/2}$ (and therefore

Σ^{-1}) may not be unique. The following fact about Gaussian distributions is useful. The proof is based on the singular value decomposition and is deferred to Appendix C.

Lemma 1. *For a set of vector random variables $\mathbf{X}, \mathbf{Y}, \mathbf{Z}$, there exist invertible linear transforms $\mathbf{X} \mapsto \bar{\mathbf{X}}, \mathbf{Y} \mapsto \bar{\mathbf{Y}}, \mathbf{Z} \mapsto \bar{\mathbf{Z}}$ such that all the five covariance matrices $\Sigma_{\bar{\mathbf{X}}}, \Sigma_{\bar{\mathbf{Y}}}, \Sigma_{\bar{\mathbf{Z}}}, \Sigma_{\bar{\mathbf{X}}\bar{\mathbf{Y}}}, \Sigma_{\bar{\mathbf{X}}\bar{\mathbf{Z}}}$ are diagonalized if and only if \mathbf{G} commutes with \mathbf{H} where*

$$\mathbf{G} := \Sigma_{\mathbf{X}}^{-1/2} \Sigma_{\mathbf{X}\mathbf{Y}} \Sigma_{\mathbf{Y}}^{-1} \Sigma_{\mathbf{Y}\mathbf{X}} \Sigma_{\mathbf{X}}^{-1/2}, \quad (33)$$

$$\mathbf{H} := \Sigma_{\mathbf{X}}^{-1/2} \Sigma_{\mathbf{X}\mathbf{Z}} \Sigma_{\mathbf{Z}}^{-1} \Sigma_{\mathbf{Z}\mathbf{X}} \Sigma_{\mathbf{X}}^{-1/2}. \quad (34)$$

Remark 4. The linear transforms being invertible ensures $\mathcal{R}(\mathbf{X}, \mathbf{Y}, \mathbf{Z}) = \mathcal{R}(\bar{\mathbf{X}}, \bar{\mathbf{Y}}, \bar{\mathbf{Z}})$.

Remark 5. For Hermitian matrices \mathbf{A} and \mathbf{B} of the same dimensions, we write $\mathbf{A} \preceq \mathbf{B}$ if $\mathbf{B} - \mathbf{A}$ is positive-semidefinite. From the positive definiteness of covariance matrices it's straightforward to show that $\mathbf{0} \preceq \mathbf{G} \preceq \mathbf{I}$ and $\mathbf{0} \preceq \mathbf{H} \preceq \mathbf{I}$, where \mathbf{G} and \mathbf{H} are defined in (33) and (34). Indeed \mathbf{G} and \mathbf{H} take the roles of ρ_{XY}^2 and ρ_{XZ}^2 in the scalar Gaussian case.

Remark 6. If X^n, Y^n and Z^n are drawn from jointly stationary Gaussian processes, then the commutativity assumption in the lemma is satisfied approximately for n large. This is due to the commutativity of convolution.

Corollary 1. *If \mathbf{X} and \mathbf{Y} are jointly Gaussian vectors, then there exist invertible linear transforms $\mathbf{X} \mapsto \bar{\mathbf{X}}$ and $\mathbf{Y} \mapsto \bar{\mathbf{Y}}$ such that $\Sigma_{\bar{\mathbf{X}}}, \Sigma_{\bar{\mathbf{Y}}}$ and $\Sigma_{\bar{\mathbf{X}}\bar{\mathbf{Y}}}$ are diagonalized.*

Thanks to Corollary 1, the task of finding the key capacity of arbitrarily correlated Gaussian vector sources in the absence of an eavesdropper is reduced to the case of product Gaussian sources (X^L, Y^L) satisfying (1) and (2). Note that assuming \mathbf{X} and \mathbf{Y} have the same length does not lose generality since one can always pad zero coordinates to \mathbf{X} and \mathbf{Y} so that they have the same length. In the presence of an eavesdropper, it is not always possible to reduce the problem to the case of product sources, since the commutativity condition in Lemma 1 is not always fulfilled; we discuss its practical relevance later in III-C.

Proof of Theorem 2: Reference [3] derived an explicit formula for the achievable key rate in the case of scalar Gaussian sources, which, in our notations, can be expressed as

$$R(r) = \frac{1}{2} \log(1 + \beta^+ - \beta^+ \exp(-2r)) \quad (35)$$

where $\beta := \frac{\rho_{xy}^2 - \rho_{xz}^2}{1 - \rho_{xy}^2}$ and $\beta^+ := \max\{\beta, 0\}$. The bases of log and exp in (35) depend on the unit of the information rates (e.g. bits or nats).

Now consider the product sources, and suppose that (r_1^*, \dots, r_L^*) achieves the maximum in (20). According to Theorem 3, either $R'_i(r_i^*) = \frac{\beta_i^+ \exp(-2r_i^*)}{1 + \beta_i^+ - \beta_i^+ \exp(-2r_i^*)} = \mu$ or $r_i^* = 0$ for each i , where μ is some constant. For fixed μ , this means

$$r_i^* = \max \left\{ 0, \frac{1}{2} \log \frac{(1 + \mu)\beta_i^+}{\mu(1 + \beta_i^+)} \right\}. \quad (36)$$

Equivalently, we can write

$$r_i^* = \frac{1}{2} \log \frac{\beta_i^+(m_i + 1)}{(\beta_i^+ + 1)m_i}, \quad (37)$$

where $m_i := \min\{\mu, \beta_i^+\}$. The claim then follows by substituting the value of r_i^* into (35) and applying (20). ■

B. Secret Key per Bit of Communication

Fix P_{XYZ} . The secret key per bit of communication is defined as

$$\eta_Z(X; Y) := \sup_{r>0} \frac{R(r)}{r}. \quad (38)$$

From the convexity of the achievable rate region one immediately sees that $\eta_Z(X; Y) := \lim_{r \rightarrow 0} \frac{R(r)}{r}$.

Define

$$s_Z^*(X; Y) := \sup_{U, V} \frac{I(V; Y|U) - I(V; Z|U)}{I(V; X|U) - I(V; Z|U) + I(U; X) - I(U; Y)}, \quad (39)$$

where the supremum is over all (U, V) such that $(U, V) - X - (Y, Z)$ form a Markov chain and that the denominator in (39) does not vanish. Note that the denominator is always nonnegative; if it vanishes for all U, V , then so does the numerator and we set $s_Z^*(X; Y) = 0$. From (39) and (16) it is immediate to see how $s_Z^*(X; Y)$ is related to $\eta_Z(X; Y)$. In the special case of no eavesdropper, this is related to the result in [12], which uses the incorrect constant $\rho_m^2(X; Y)$ as we mentioned earlier.

Theorem 3. *Secret key per bit of communication is linked to $s_Z^*(X; Y)$ by*

$$\eta_Z(X; Y) = \frac{s_Z^*(X; Y)}{1 - s_Z^*(X; Y)}. \quad (40)$$

Proof: The characterization of $\mathcal{R}(X, Y, Z)$ is given in (16). Thus $\sup_{r>0} \frac{R(r)}{r} = \frac{s_Z^*(X; Y)}{1 - s_Z^*(X; Y)}$ follows immediately from the definition of $s_Z^*(X; Y)$. The claim of $\lim_{r \downarrow 0} \frac{R(r)}{r} = \sup_{r>0} \frac{R(r)}{r}$ follows from the convexity of the achievable rate region. ■

The following results provide some basic properties of $s_Z^*(X; Y)$. The rationale for defining $s_Z^*(X; Y)$ can be explained by Theorem 3 and 6) in Theorem 4.

Theorem 4 (Properties of $s_Z^*(X; Y)$).

1) *For any P_{XYZ} ,*

$$0 \leq s_Z^*(X; Y) \leq 1. \quad (41)$$

2) *For product sources (X^L, Y^L, Z^L) as in (1) and (2),*

$$s_{Z^L}^*(X^L; Y^L) = \max_{1 \leq i \leq L} s_{Z_i}^*(X_i; Y_i). \quad (42)$$

3) *For arbitrary $P_{XYZ} = P_X P_{Y|X}$,*

$$s_Z^*(X; Y) = \sup_{Q_{V|X}} \frac{I(\bar{V}; \bar{Y}) - I(\bar{V}; \bar{Z})}{I(\bar{V}; \bar{X}) - I(\bar{V}; \bar{Z}) + D(Q_X \| P_X) - D(Q_Y \| P_Y)}, \quad (43)$$

where $\bar{V}, \bar{X}, \bar{Y}, \bar{Z}$ have the joint distribution

$$P_{\bar{V}\bar{X}\bar{Y}\bar{Z}}(v, x, y, z) = Q_{VX}(v, x)P_{YZ|X}(y, z|x). \quad (44)$$

The supremum is over all Q_{VX} such that the above denominator does not vanish.

Computation can be further simplified when the source has certain structures:

- 4) If P_{XYZ} is stochastically degraded,

$$\begin{aligned} s_Z^*(X; Y) &= \sup_U \frac{I(U; Y|Z)}{I(U; X|Z)} \\ &= \sup_{Q_X} \frac{D(Q_Y||P_Y) - D(Q_Z||P_Z)}{D(Q_X||P_X) - D(Q_Z||P_Z)} \end{aligned} \quad (45)$$

where $Q_{XYZ} = Q_X P_{YZ|X}$.

- 5) As a special case of (45), if $X = (X', Z)$, $Y = (Y', Z)$, then

$$s_Z^*(X; Y) = \text{ess sup}_{z \in \mathcal{Z}} s^*(X'; Y'|Z = z), \quad (46)$$

where ess sup denotes the essential supremum of a real valued function.

- 6) If Z is constant, we recover $s_Z^*(X; Y) = s^*(X; Y)$, which is the best constant for the strong data processing inequality defined in (6).

Proof: See Appendix B. ■

Remark 7. The interpretation of the tensorization of $s_Z^*(X; Y)$ in (42) is that, with small allowable public communication, it is always efficient to only use the best component of the product sources. Alternatively, the fact that rate splitting is optimal for product sources implies the tensorization property of $s_Z^*(X; Y)$.

Remark 8. If the source is stochastically degraded, then $s_Z(X; Y)$ can be computed from (45) which only requires optimizing over an auxiliary distribution Q_X , instead of the optimization over a family of distributions $P_{U|X}$ when computing the rate region via (19). Similarly for non-degraded sources, (43) only involves optimizing over Q_{VX} whereas the region rate region (16) requires optimizing over $P_{UV|X}$. Thus, in either case, the optimization problem may be considerably reduced if one is only interested in $\eta_Z(X; Y)$ instead of the whole rate region.

Example 1 (Symmetric Bernoulli Source). Suppose X, Y and Z are symmetric Bernoulli random variables, with $\epsilon_{XY} := \mathbb{P}[X \neq Y]$ and $\epsilon_{XZ} := \mathbb{P}[X \neq Z]$ satisfying $\epsilon_{XY} \leq \epsilon_{XZ} < \frac{1}{2}$. The achievable region $\mathcal{R}(X, Y, Z)$ was derived in [22], from which one can obtain

$$\eta_Z(X; Y) = \frac{(1 - 2\epsilon_{XY})^2 - (1 - 2\epsilon_{XZ})^2}{1 - (1 - 2\epsilon_{XY})^2}. \quad (47)$$

Since X, Y , and Z are stochastically degraded, we can assume without loss of generality that $X - Y - Z$ form a Markov chain, and use (40) and (45) to obtain (47). In this case (45) is supremized as Q_X approaches the equiprobable distribution on $\{0, 1\}$.

Example 2 (Scalar Gaussian Source). Setting $L = 1$ in Theorem 2 gives

$$\eta_Z(X; Y) = \beta \quad (48)$$

where

$$\beta := \frac{\rho_{XY}^2 - \rho_{XZ}^2}{1 - \rho_{XY}^2} \quad (49)$$

for jointly Gaussian random variables X, Y and Z satisfying $\rho_{XZ} \leq \rho_{XY} < 1$. We remark that the (less trivial) direction of $\eta_Z(X; Y) \leq \beta$ can also be expected from Example 1 (whereas the proof of this direction using Theorem 2 essentially relies on entropy power inequality buried in Fact 1); see Appendix D.

Example 3 (Product Gaussian Source). If \mathbf{X}, \mathbf{Y} and \mathbf{Z} are as in Theorem 2, then

$$\eta_Z(\mathbf{X}; \mathbf{Y}) = \max_{1 \leq i \leq L} \beta_i^+, \quad (50)$$

where β_i is as in Theorem 2.

In addition to the potential dimension reduction in numerical evaluations (see Remark 8), another important motivation for considering $\eta_Z(X; Y)$ is that there exist source distributions for which $\eta_Z(X; Y)$ can be computed analytically even though $\mathcal{R}(X, Y, Z)$ is not completely known, as epitomized by the case of vector Gaussian sources in Theorem 5 below. Note that Theorem 5 holds even when the commutativity in Lemma 1 fails. The achievability (lower bound) part of Theorem 5 is accomplished by choosing an appropriate sequence of Q_{VX} in (43) followed by routine computations; the converse part requires slightly more ingenuity: we construct a new source distribution $P_{XY\hat{Z}}$ satisfying $\mathcal{R}(X, Y, Z) \subseteq \mathcal{R}(X, Y, \hat{Z})$, but for which the commutativity in Lemma 1 is fulfilled and $\eta_{\hat{Z}}(X; Y) = \eta_Z(X; Y)$. Details of the proof are relegated to Appendix E.

Theorem 5. If \mathbf{X}, \mathbf{Y} and \mathbf{Z} in the key generation model are jointly Gaussian vectors, then

$$\eta_Z(\mathbf{X}; \mathbf{Y}) = \lambda_{\max}^+((\mathbf{G} - \mathbf{H})(\mathbf{I} - \mathbf{G})^{-1}), \quad (51)$$

where $\lambda_{\max}(\cdot)$ and $\lambda_{\min}(\cdot)$ denote the largest and smallest eigenvalues of a matrix, and recall the notation $\lambda_{\max}^+ := \max\{0, \lambda_{\max}\}$.

C. Key-Communication Function for Stationary Gaussian Processes

We now derive the key-rate-communication-rate tradeoff for stationary Gaussian processes $(\mathbb{X}, \mathbb{Y}, \mathbb{Z})$. In contrast to the setting of product sources since in this section we deal with sources with memory. However as mentioned in Remark 6, one can still apply Lemma 1, and in fact the linear transforms can be easily found. Let us discuss the intuitions before diving into the formal proof. As a first attempt, it is tempting to pick the Fourier transform as the invertible linear transforms in Lemma 1, since it diagonalizes circulant matrices [23]. However this is not an allowable choice, since the linear transforms in Lemma 1 are real, thereby excluding the Fourier transform. In general, complex linear transforms are not useful

for the conversion to product sources, since complex Gaussian variables may not be independent even if their correlation coefficient is zero.

The Fourier transform, however, is not too far from the correct choice. If a circulant matrix is symmetric, we can also diagonalize it with the sine/cosine orthogonal matrix (to be defined soon). In general, the cross-correlations R_{XY} and R_{XZ} are not symmetric, so the trick is to first pass \mathbb{Y} through a filter whose impulse response is R_{XY}^7 , the correlation function between \mathbb{X} and \mathbb{Y} , resulting in a new process $\hat{\mathbb{Y}}$. Similarly, we construct $\hat{\mathbb{Z}}$ by convolving with R_{XZ} yielding

$$R_{X\hat{Y}} = R_{XY} * R_{YX}, \quad (52)$$

$$R_{X\hat{Z}} = R_{XZ} * R_{ZX}, \quad (53)$$

which are symmetric functions. Set $\bar{\mathbf{X}} = \mathbf{Q}^\top X^n$, $\bar{\mathbf{Y}} = \mathbf{Q}^\top \hat{\mathbf{Y}}^n$, $\bar{\mathbf{Z}} = \mathbf{Q}^\top \hat{\mathbf{Z}}^n$ where \mathbf{Q} the sine/cosine orthogonal matrix, i.e., for $1 \leq k, l \leq n$,

$$Q_{kl} := \begin{cases} \cos(\frac{2\pi}{n} \lfloor \frac{l}{2} \rfloor k) & l \text{ is odd;} \\ \sin(\frac{2\pi}{n} \lfloor \frac{l}{2} \rfloor k) & l \text{ is even.} \end{cases} \quad (54)$$

Then the covariance matrices $\Sigma_{\bar{\mathbf{X}}}$, $\Sigma_{\bar{\mathbf{Y}}}$, $\Sigma_{\bar{\mathbf{Z}}}$, $\Sigma_{\bar{\mathbf{X}}\bar{\mathbf{Y}}}$, $\Sigma_{\bar{\mathbf{X}}\bar{\mathbf{Z}}}$ will be asymptotically diagonal as their dimension grows.

In summary, the original Gaussian sources are converted to sources satisfying the product assumption (1) and (2) in the spectral representation, and the correlation coefficients corresponding to frequency ω (which relates to the factor $\frac{2\pi}{n} \lfloor \frac{l}{2} \rfloor$ in (54)) are

$$\rho_{XY}(\omega) := \frac{|S_{XY}(\omega)|}{\sqrt{S_X(\omega)S_Y(\omega)}}, \quad (55)$$

$$\rho_{XZ}(\omega) := \frac{|S_{XZ}(\omega)|}{\sqrt{S_X(\omega)S_Z(\omega)}}, \quad (56)$$

where $S_X, S_Y, S_Z, S_{XY}, S_{XZ}$ denote the spectral densities and joint spectral densities. From (55), (56) and Theorem 2, we can anticipate the expression in the next result. To prove it rigorously we impose a technical condition that requires all correlations and cross-correlations to be absolutely summable (that is, the corresponding spectrum functions are in the ‘‘Wiener class’’ [23]). We do not believe this condition to be crucial for the validity of the result.

Theorem 6. Suppose \mathbb{X}, \mathbb{Y} and \mathbb{Z} are Wiener class stationary Gaussian processes, and

$$\beta(\omega) := \frac{|S_{XY}(\omega)|^2 S_Z(\omega) - |S_{XZ}(\omega)|^2 S_Y(\omega)}{S_X(\omega) S_Y(\omega) S_Z(\omega) - |S_{XY}(\omega)|^2 S_Z(\omega)} \quad (57)$$

is well-defined, that is, excluding the 0/0 case. Then the achievable communication and key rates are parameterized

⁷When R_{XY} is strictly bandlimited, convolution with R_{XY} becomes a degenerate linear transform. In this case we can use a signal \hat{R}_{XY} as an alternative, where \hat{R}_{XY} has full spectrum and agrees with R_{XY} in the pass-band of R_{XY} . The final formula of key capacity however will remain unchanged.

by $\mu > 0$ as

$$r = \frac{1}{4\pi} \int_{\beta(\omega) > \mu} \log \frac{\beta(\omega)(\mu + 1)}{(\beta(\omega) + 1)\mu} d\omega, \quad (58)$$

$$R = \frac{1}{4\pi} \int_{\beta(\omega) > \mu} \log \frac{\beta(\omega) + 1}{\mu + 1} d\omega. \quad (59)$$

Remark 9.

$$\eta_{\mathbb{Z}}(\mathbb{X}; \mathbb{Y}) = \sup_{\omega \in [0, 2\pi)} (\beta^+(\omega)). \quad (60)$$

Remark 10. From (55) and (56) we can verify that

$$\beta(\omega) = \frac{\rho_{XY}^2(\omega) - \rho_{XZ}^2(\omega)}{1 - \rho_{XY}^2(\omega)}, \quad (61)$$

which is the counterpart of β_i in Theorem 2.

The achievability proof of Theorem 6 is given in Sections IV and V, and the converse is relegated to Appendix H.

IV. ACHIEVABILITY OF ONE-SHOT KEY GENERATION

The single-letter expressions of (16) or (19) only apply to discrete memoryless sources. In order to allow memory, and in particular to prove the achievability part of Theorem 6, we derive a one-shot achievability result in this section. The proof relies on a stochastic encoding scheme called *likelihood encoder* [21]. The idea is to introduce an idealized distribution which is easier to work with, and which approximates the true distribution in total variation distance under certain rate conditions according to soft covering lemma/resolvability [24].

Notation 1. Given P_{XY} , denote the information density by

$$i_{X;Y}(x; y) := \log \frac{dP_{XY}}{d(P_X \times P_Y)}(x, y). \quad (62)$$

Theorem 7. Suppose the sources are distributed according to P_{XYZ} , the integers $M, M_1, M_2 > 0$, and $\bar{P}_{U|X}$ is a conditional distribution on an arbitrary alphabet \mathcal{U} . Then there is a scheme such that $|\mathcal{W}| = M$, $|\mathcal{K}| = M_1$, and that

$$\mathbb{P}(\hat{K} \neq K) \leq \epsilon^*, \quad (63)$$

$$\log M_1 - H(K|WZ) \leq \inf_{0 < \delta < e^{-1} M_1^{\frac{3}{2}}} \left\{ (T^* + 8\delta) \log \frac{M_1^{\frac{3}{2}}}{\delta} \right\}, \quad (64)$$

where ϵ^* and T^* are defined in (111) and (112).

Proof: Fix the joint distribution of the sources P_{XYZ} . Let $\bar{P}_{U|XYZ} = \bar{P}_{U|X} P_{XYZ}$. Randomly generate a codebook

$$\mathbf{U} \in \mathcal{U}^{M \times M_1 \times M_2} \quad (65)$$

according to \bar{P}_U . Let P_{WKLXYZ} be the distribution induced by the likelihood encoder [21]:

$$P_{WKL|XYZ}(w, k, l|x, y, z) = \frac{1}{Z_x} \bar{P}_{X|U}(x|U(w, k, l)) \quad (66)$$

where Z_x is a normalization constant independent of (w, k, l) . In words, the stochastic encoder in (66) outputs the indices

w , k and l according to the likelihood of $U(w, k, l)$ passing through the “test channel” $\bar{P}_{X|U}$. Define

$$Q_{XWKL}(x, w, k, l) = \frac{1}{MM_1M_2} \bar{P}_{X|U}(x|U(w, k, l)), \quad (67)$$

$$Q_{YZ|XWKL} = P_{YZ|X}. \quad (68)$$

Note that Q_{WKL} is an equiprobable distribution, hence by the construction of the likelihood encoder we have

$$P_{WKL|X} = Q_{WKL|X}. \quad (69)$$

We now digress into a brief review of the *total variation distance*. By definition, the total variation distance between probability measures P and Q on the same σ -algebra of subsets \mathcal{F} of the sample space \mathcal{X} is

$$|P - Q| := \sup_{A \in \mathcal{F}} |P(A) - Q(A)|. \quad (70)$$

Below are some of the relevant properties of total variational distance; see for example [24].

Property 1. 1) Triangle inequality: if P , Q and S are distributions on the same sample space, then

$$|P - Q| \leq |P - S| + |S - Q|. \quad (71)$$

2) If $P_X P_{Y|X}$ and $Q_X Q_{Y|X}$ are joint distributions on $\mathcal{X} \times \mathcal{Y}$, then

$$|P_X - Q_X| \leq |P_X P_{Y|X} - Q_X Q_{Y|X}| \quad (72)$$

where the equality holds when $P_{Y|X} = Q_{Y|X}$.

According to Theorem VII.1 in [24], we have the following bounds on the total variations with respect to the codebook \mathcal{C} :

$$\mathbb{E}_{\mathcal{C}} |Q_{Z|W=w} - P_Z| \leq T_1, \quad (73)$$

$$\mathbb{E}_{\mathcal{C}} |Q_{Z|W=w, K=k} - P_Z| \leq T_2, \quad (74)$$

for each m, k , where

$$T_1 := \inf_{\tau > 0} \left\{ \mathbb{P}[\imath_{U;Z}(U; Z) > \tau] + \frac{1}{2} \sqrt{\frac{2\tau}{MM_2}} \right\}, \quad (75)$$

$$T_2 := \inf_{\tau > 0} \left\{ \mathbb{P}[\imath_{U;Z}(U; Z) > \tau] + \frac{1}{2} \sqrt{\frac{2\tau}{M_2}} \right\}, \quad (76)$$

and $\imath_{U;Z}(U; Z)$ is computed with the joint distribution \bar{P}_{UZ} . By the triangle inequality,

$$\mathbb{E}_{\mathcal{C}} |Q_{Z|W=w, K=k} - Q_{Z|W=w}| \leq T_1 + T_2, \quad \forall w, k, \quad (77)$$

and since $Q_{WK} = Q_W Q_K$, we obtain

$$\begin{aligned} \mathbb{E}_{\mathcal{C}} |Q_{ZWK} - Q_{ZW} Q_K| &= \mathbb{E}_{\mathcal{C}} |Q_{ZWK} - Q_{Z|W} Q_{WK}| \quad (78) \\ &\leq T_1 + T_2. \quad (79) \end{aligned}$$

From $P_{WKL|X} = Q_{WKL|X}$, we have

$$\mathbb{E}_{\mathcal{C}} |P_{WKLX} - Q_{WKLX}| = \mathbb{E}_{\mathcal{C}} |P_X - Q_X| \quad (80)$$

$$\leq T_3, \quad (81)$$

where

$$T_3 := \inf_{\tau > 0} \left\{ \mathbb{P}[\imath_{U;X}(U; X) > \tau] + \frac{1}{2} \sqrt{\frac{2\tau}{MM_1M_2}} \right\} \quad (82)$$

and $\imath_{U;X}(U; X)$ is computed with the joint distribution \bar{P}_{UX} . Therefore by (68),

$$\mathbb{E}_{\mathcal{C}} |P_{KWZ} - Q_{KWZ}| \leq \mathbb{E}_{\mathcal{C}} |P_{KWZX} - Q_{KWZX}| \quad (83)$$

$$= \mathbb{E}_{\mathcal{C}} |P_{KWX} - Q_{KWX}| \quad (84)$$

$$\leq T_3, \quad (85)$$

and

$$\mathbb{E}_{\mathcal{C}} |P_{WZ} Q_K - Q_{WZ} Q_K| = \mathbb{E}_{\mathcal{C}} |P_{WZ} - Q_{WZ}| \leq T_3. \quad (86)$$

Equations (78), (85), (86) and the triangle inequality imply that

$$\begin{aligned} \mathbb{E}_{\mathcal{C}} \int |P_{K|ZW} - Q_K| dP_{ZW} &= \mathbb{E}_{\mathcal{C}} |P_{KWZ} - P_{ZW} Q_K| \quad (87) \\ &\leq T_1 + T_2 + 2T_3. \quad (88) \end{aligned}$$

Lemma 2. For any z, w ,

$$\begin{aligned} D(P_{K|Z=z, W=w} || Q_K) \\ \leq 2 |P_{K|Z=z, W=w} - Q_K| \log \frac{M_1^{\frac{3}{2}}}{|P_{K|Z=z, W=w} - Q_K|}. \quad (89) \end{aligned}$$

Proof:

$$\begin{aligned} D(P_{K|Z=z, W=w} || Q_K) \\ = -H(P_{K|Z=z, W=w}) + \sum_{k=1}^{M_1} P_{K|Z=z, W=w}(k) \log \frac{1}{Q_K(k)} \quad (90) \end{aligned}$$

$$\begin{aligned} &= -H(P_{K|Z=z, W=w}) + H(Q_K) \\ &+ \sum_{k=1}^{M_1} (P_{K|Z=z, W=w}(k) - Q_K(k)) \log M_1 \quad (91) \end{aligned}$$

$$\begin{aligned} &\leq 2 |P_{K|Z=z, W=w} - Q_K| \log \frac{M_1}{|P_{K|Z=z, W=w} - Q_K|} \\ &+ |P_{K|Z=z, W=w} - Q_K| \log M_1, \quad (92) \end{aligned}$$

where the last step used the inequality in [25]. \blacksquare

Thanks to the lemma, for any $0 < \delta < e^{-1} M_1^{\frac{3}{2}}$ we have

$$\begin{aligned} I(K; Z, W) \\ = D(P_{KZW} || P_K P_{ZW}) \quad (93) \end{aligned}$$

$$\leq D(P_{KZW} || Q_K P_{ZW}) \quad (94)$$

$$= \int D(P_{K|ZW} || Q_K) dP_{ZW} \quad (95)$$

$$\leq 2 \int |P_{K|ZW} - Q_K| \log \frac{M_1^{\frac{3}{2}}}{|P_{K|ZW} - Q_K|} dP_{ZW} \quad (96)$$

$$= 2 \log M_1^{\frac{3}{2}} |P_{KZW} - Q_K P_{ZW}| \quad (97)$$

$$+ 2 \int |P_{K|ZW} - Q_K| \log \frac{1}{|P_{K|ZW} - Q_K|} dP_{ZW} \quad (98)$$

$$\leq 2 |P_{KZW} - Q_K P_{ZW}| \left(\log M_1^{\frac{3}{2}} + \log \frac{1}{|P_{KZW} - Q_K P_{ZW}|} \right) \quad (99)$$

$$\leq 2 \log \frac{M_1^{\frac{3}{2}}}{\delta} (|P_{KZW} - Q_K P_{ZW}| + \delta), \quad (100)$$

where we used Jensen's inequality in (99) and $x \log \frac{\lambda}{x} \leq (x + \delta) \log \frac{\lambda}{\delta}$ for all $x > 0$ and $0 < \delta < e^{-1}\lambda$ in (100). Averaging (100) over the codebook and applying (88), we obtain

$$\mathbb{E}_{\mathcal{C}} I(K; Z, W) \leq 2 \log \frac{M_1^{\frac{3}{2}}}{\delta} (T_1 + T_2 + 2T_3 + \delta). \quad (101)$$

Similarly from (85) we have $\mathbb{E}_{\mathcal{C}} |P_K - Q_K| \leq T_3$, hence

$$\mathbb{E}_{\mathcal{C}} [\log K - H(K)] = \mathbb{E}_{\mathcal{C}} D(P_K \| Q_K) \leq 2 \log \frac{M_1^{\frac{3}{2}}}{\delta} (T_3 + \delta). \quad (102)$$

Thus for the security constraint, we have

$$\mathbb{E}_{\mathcal{C}} [\log K - H(K|WZ)] \leq 2 \log \frac{M_1^{\frac{3}{2}}}{\delta} (T_1 + T_2 + 3T_3 + 2\delta), \quad (103)$$

which follows from (101) and (102).

For the key agreement constraint, choose a good channel decoder $P_{\hat{K}|WY}$, and let

$$P_{WKLXYZ\hat{W}} = P_{WKLXYZ} P_{\hat{K}|WY}, \quad (104)$$

$$Q_{WKLXYZ\hat{W}} = Q_{WKLXYZ} P_{\hat{K}|WY}. \quad (105)$$

Then using a single-shot version of Shannon's achievability bound [26] for discrete memoryless channels, the error probability of the channel decoder can be bounded as $\mathbb{E}_{\mathcal{C}} \mathbb{P}_Q(\hat{K} \neq K) \leq \epsilon$ where we have defined

$$\epsilon := \inf_{\gamma > 0} \{ \mathbb{P}[\mathfrak{u}_{U;Y}(U; Y) \leq \log(M_1 M_2 - 1) + \gamma] + \exp(-\gamma) \}, \quad (106)$$

and $\mathfrak{u}_{U;Y}(U; Y)$ is computed with the joint distribution \bar{P}_{UY} . Then, the probability of decoding K erroneously under the true distribution is bounded as

$$\mathbb{E}_{\mathcal{C}} \mathbb{P}_P(\hat{K} \neq K) \leq \mathbb{E}_{\mathcal{C}} \mathbb{P}_Q(\hat{K} \neq K) + |P_X - Q_X| \quad (107)$$

$$\leq T_3 + \epsilon, \quad (108)$$

where \mathbb{P}_P and \mathbb{P}_Q denote the probabilities under the distributions P_{XYWK} and Q_{XYWK} , respectively. In (107) we used $P_{K\hat{K}WY|X} = Q_{K\hat{K}WY|X}$, which follows from $P_{WY|X} = Q_{WY|X}$ in (69), and that K and \hat{K} are functions of X and (W, Y) , respectively. By Markov's inequality,

$$\mathbb{P}_{\mathcal{C}}[\mathbb{P}_P(\hat{K} \neq K) > 2(T_3 + \epsilon)] < \frac{1}{2}. \quad (109)$$

Similarly from (103),

$$\begin{aligned} \mathbb{P}_{\mathcal{C}} \left[\log K - H(K|WZ) > 4(T_1 + T_2 + 3T_3 + 2\delta) \log \frac{M_1^{\frac{3}{2}}}{\delta} \right] \\ < \frac{1}{2}. \end{aligned} \quad (110)$$

Hence there exists a codebook which satisfies the properties in Theorem 7 where

$$\epsilon^* := 2(T_3 + \epsilon), \quad (111)$$

$$T^* := 4(T_1 + T_2 + 3T_3); \quad (112)$$

and T_1, T_2, T_3, ϵ are as in (75), (76), (82) and (106). ■

V. APPROXIMATION OF GAUSSIAN PROCESSES AND ACHIEVABILITY OF THEOREM 6

In this section we apply Theorem 7 to stationary Gaussian processes to finish the achievability part of Theorem 6. The derivation is essentially based on the asymptotic distribution of the eigenvalues of Toeplitz matrices, a brief review of which is given in Appendix I.

We now introduce notations for Toeplitz matrices and circulant matrices. Given a continuous function f on $[0, 2\pi)$, define for $k = 0, 1, \dots, n-1$,

$$t_k := \frac{1}{2\pi} \int_0^{2\pi} f(\omega) e^{ik\omega} d\omega, \quad (113)$$

$$c_k^{(n)} := \sum_{m=-\infty}^{\infty} t_{-k+mn}. \quad (114)$$

Note that from (114), an equivalent way of defining $c_k^{(n)}$ is

$$c_k^{(n)} := \frac{1}{n} \sum_{j=0}^{n-1} f(2\pi j/n) e^{2\pi ijk/n}. \quad (115)$$

If $\{t_k\}$ has fast decay, then $\{c_k^{(n)}\}$ approximates $\{t_k\}$ for large n . The advantage of $\{c_k^{(n)}\}$ over $\{t_k\}$ is that the former is a periodic sequence. For $0 \leq i, j \leq n-1$, define

$$[\mathbf{T}_n(f)]_{i,j} := t_{i-j}, \quad (116)$$

$$[\mathbf{C}_n(f)]_{i,j} := c_{i-j}^{(n)}. \quad (117)$$

Then it is clear that (117) is a circulant matrix.

Using the above notations, the covariance matrix of the vector (X^n, Y^n, Z^n) which are samples from $(\mathbb{X}, \mathbb{Y}, \mathbb{Z})$ can be expressed as

$$\mathbf{T}_n := \begin{pmatrix} \mathbf{T}_n(S_X) & \mathbf{T}_n(S_{XY}) & \mathbf{T}_n(S_{XZ}) \\ \mathbf{T}_n(S_{YX}) & \mathbf{T}_n(S_Y) & \mathbf{T}_n(S_{YZ}) \\ \mathbf{T}_n(S_{ZX}) & \mathbf{T}_n(S_{ZY}) & \mathbf{T}_n(S_Z) \end{pmatrix}, \quad (118)$$

$$(119)$$

Now define a positive-semidefinite matrix composed of circulant blocks

$$\mathbf{C}_n := \begin{pmatrix} \mathbf{C}_n(S_X) & \mathbf{C}_n(S_{XY}) & \mathbf{C}_n(S_{XZ}) \\ \mathbf{C}_n(S_{YX}) & \mathbf{C}_n(S_Y) & \mathbf{C}_n(S_{YZ}) \\ \mathbf{C}_n(S_{ZX}) & \mathbf{C}_n(S_{ZY}) & \mathbf{C}_n(S_Z) \end{pmatrix}. \quad (120)$$

We assume that all the spectrums belong to the Wiener class. Then from Fact 4 in Appendix I we have

$$\mathbf{T}_n \sim \mathbf{C}_n \quad (121)$$

since the corresponding blocks in \mathbf{T}_n and \mathbf{C}_n are asymptotically equivalent. We shall use \mathbf{C}_n as a proxy for \mathbf{T}_n in the subsequent analysis. Let $(\tilde{X}^n, \tilde{Y}^n, \tilde{Z}^n)$ be a zero mean Gaussian vector with covariance matrix \mathbf{C}_n . Suppose \mathbf{Q} is the sin/cosine orthogonal matrix (see (54)). Define

$$\hat{\mathbf{X}} = \mathbf{Q}^\top \tilde{\mathbf{X}}, \quad (122)$$

$$\hat{\mathbf{Y}} = \mathbf{Q}^\top \mathbf{C}_n \begin{pmatrix} S_{XY} \\ |S_{XY}| \end{pmatrix} \tilde{\mathbf{Y}}, \quad (123)$$

$$\hat{\mathbf{Z}} = \mathbf{Q}^\top \mathbf{C}_n \begin{pmatrix} S_{XZ} \\ |S_{XZ}| \end{pmatrix} \tilde{\mathbf{Z}}. \quad (124)$$

Here $\frac{S_{XY}(\omega)}{|S_{XY}(\omega)|}$ can be arbitrarily set to 1 if $S_{XY}(\omega) = 0$. This ensures that $\mathbf{C}_n(\frac{S_{XY}(\omega)}{|S_{XY}(\omega)|})$ is an invertible, and in particular, unitary matrix. Note that the simplified discussion in III-C corresponds to replacing $\mathbf{C}_n(\frac{S_{XY}(\omega)}{|S_{XY}(\omega)|})$ in (123) with $\mathbf{C}_n(S_{XY})$, which may be singular. One can verify that $(\hat{\mathbf{X}}, \hat{\mathbf{Y}}, \hat{\mathbf{Z}})$ has the product structure of (1) and (2). Next we shall specify an auxiliary distribution $P_{\hat{\mathbf{U}}|\hat{\mathbf{X}}}$. We first design the correlation coefficients $\rho_{UX} : [0, 2\pi) \rightarrow [0, 1]$ as

$$\rho_{UX}(\omega) = \begin{cases} \left(\frac{(1+\mu)\rho_{XY}^2(\omega) - \rho_{XZ}^2(\omega) - \mu}{\rho_{XY}^2(\omega) - (1+\mu)\rho_{XZ}^2(\omega) + \mu\rho_{XY}^2(\omega)\rho_{XZ}^2(\omega)} \right)^{\frac{1}{2}} & \beta(\omega) > \mu \\ 0 & \text{otherwise} \end{cases} \quad (125)$$

for $\omega \in [0, 2\pi)$, where $\rho_{XY}^2(\omega)$ and $\rho_{XZ}^2(\omega)$ are as in (55) and (56). The definition (125) ensures that ρ_{UX} satisfies

$$\log \frac{\beta(\omega)(\mu+1)}{(\beta(\omega)+1)\mu} = \log \frac{1}{1-\rho_{UX}^2(\omega)} - \log \frac{1}{1-\rho_{UX}^2(\omega)\rho_{XY}^2(\omega)} \quad (126)$$

and

$$\log \frac{\beta(\omega)+1}{\mu+1} = \log \frac{1}{1-\rho_{UX}^2(\omega)\rho_{XY}^2(\omega)} - \log \frac{1}{1-\rho_{UX}^2(\omega)\rho_{XZ}^2(\omega)}. \quad (127)$$

The intuition for ρ_{UX} is as follows: suppose \mathbb{U} is a Gaussian process jointly stationary with \mathbb{X} and $\mathbb{U} - \mathbb{X} - (\mathbb{Y}, \mathbb{Z})$ such that $\frac{|S_{UX}(\omega)|}{\sqrt{S_X(\omega)S_U(\omega)}} = \rho_{UX}(\omega)$. Then from (126), (127) and Theorem 6 we can verify a counterpart of the rate region (19) for stationary processes:

$$I(\mathbb{U}; \mathbb{X}) - I(\mathbb{U}; \mathbb{Y}) = r, \quad (128)$$

$$I(\mathbb{U}; \mathbb{Y}) - I(\mathbb{U}; \mathbb{Z}) = R, \quad (129)$$

where $I(\mathbb{U}; \mathbb{X}) := \lim_{n \rightarrow \infty} \frac{1}{n} I(U^n; X^n)$ stands for the mutual information rate between \mathbb{U} and \mathbb{X} . Now, $P_{\hat{\mathbf{U}}|\hat{\mathbf{X}}_i}$ can be defined by requiring that $\hat{\mathbf{U}}_i$ is zero mean jointly Gaussian with $\hat{\mathbf{X}}_i$ satisfying

$$\rho_{\hat{\mathbf{U}}_i \hat{\mathbf{X}}_i} = \rho_{UX} \left(\frac{2\pi i}{n} \right), \quad i = 1, 2, \dots, n \quad (130)$$

The scaling of $\hat{\mathbf{U}}_i$ doesn't matter and can be chosen arbitrarily. We set $P_{\hat{\mathbf{U}}|\hat{\mathbf{X}}} = \prod_{i=1}^n P_{\hat{\mathbf{U}}_i|\hat{\mathbf{X}}_i}$. Notice that this and (122)-(124) have defined a channel $P_{\hat{\mathbf{U}}|\hat{\mathbf{X}}}$. Also beware that $\hat{\mathbf{X}}_i$ and $\hat{\mathbf{X}}_i$ (and $\bar{\mathbf{X}}_i$ to be defined later) depend implicitly on n , though \mathbf{X}_i does not. Below, $\rho_{\hat{\mathbf{U}}_i \hat{\mathbf{X}}_i}$ will be denoted by $\rho_i^{(n)}$ for simplicity.

Now for $i = 0, \dots, n-1$, define the random variables

$$\eta_i^{(n)} = \imath_{\hat{\mathbf{X}}_i; \hat{\mathbf{U}}_i}(\hat{\mathbf{X}}_i; \hat{\mathbf{U}}_i). \quad (131)$$

The following lemma will be useful later when applying Chernoff bound:

Lemma 3. Fix any $0 < \delta < \frac{1}{2}$. For any $\epsilon > 0$, there exists $t > 0$ such that

$$t\mathbb{E}\eta \leq \ln \mathbb{E}e^{t\eta} \leq (1+\epsilon)t\mathbb{E}\eta + \epsilon t \quad (132)$$

for all $\rho \in [\delta - 1, 1 - \delta]$, where $\eta := \imath_{U;X}(U; X)$, in which U, X are jointly Gaussian with correlation coefficient ρ .

Proof: See Appendix F. ■

Now return to the proof of Theorem 6. Define

$$\delta := 1 - \sup_{0 \leq \omega < 2\pi} \rho_{UX}(\omega). \quad (133)$$

From the assumption of Theorem 5, we know that $S_X(\omega)$, $S_Z(\omega)$ and $S_Z(\omega)$ do not vanish for any $\omega \in [0, 2\pi)$, since otherwise $\beta(\omega)$ will be a fraction of the type $\frac{0}{0}$ for some ω . This in turn implies that

$$\min_{0 \leq \omega < 2\pi} S_X(\omega) > 0, \quad \min_{0 \leq \omega < 2\pi} S_Y(\omega) > 0, \quad \min_{0 \leq \omega < 2\pi} S_Z(\omega) > 0; \quad (134)$$

since $S_X(\omega)$, $S_Y(\omega)$ and $S_Z(\omega)$ are continuous functions on the compact set $[0, 2\pi)$. We shall make an additional assumption that

$$\sup_{0 \leq \omega < 2\pi} \rho_{XY}^2(\omega) < 1. \quad (135)$$

Fortunately, the proof does not lose any generality due to the assumptions of (135):

Lemma 4. If Theorem 6 holds for sources satisfying (135), then it must also hold without those assumptions.

Proof: Assume that Theorem 6 is proved under the assumptions (135). For general source $(\mathbb{X}, \mathbb{Y}, \mathbb{Z})$ and $\lambda \in [0, 1]$, we can degrade \mathbb{Y} by $\mathbb{Y}^\lambda := \mathbb{Y} + \lambda\mathbb{N}$, where \mathbb{N} is a stationary white Gaussian processes such that \mathbb{N} and $(\mathbb{X}, \mathbb{Y}, \mathbb{Z})$ are independent. Let $\beta^\lambda(\omega)$ be as defined in Theorem 6 but for the new source $(\mathbb{X}, \mathbb{Y}^\lambda, \mathbb{Z})$, and define

$$r^\lambda := \frac{1}{4\pi} \int_{\beta^\lambda(\omega) > \mu} \log \frac{\beta^\lambda(\omega)(\mu+1)}{(\beta^\lambda(\omega)+1)\mu} d\omega, \quad (136)$$

$$R^\lambda := \frac{1}{4\pi} \int_{\beta^\lambda(\omega) > \mu} \log \frac{\beta^\lambda(\omega)+1}{\mu+1} d\omega. \quad (137)$$

It's easy to check that $\beta^\lambda(\omega) \uparrow \beta(\omega)$ as $\lambda \downarrow 0$ for each $\omega \in [0, 2\pi)$. Then by monotone convergence theorem we have $r^\lambda \uparrow r$ and $R^\lambda \uparrow R$ as $\lambda \downarrow 0$, where r and R are as in (58) and (59). However for each $\lambda > 0$ the condition (135) holds. By our assumption we can prove $(r^\lambda, R^\lambda) \in \mathcal{R}(\mathbb{X}, \mathbb{Y}^\lambda, \mathbb{Z})$, and the Markov chain $\mathbb{Y}^\lambda - \mathbb{Y} - (\mathbb{X}, \mathbb{Z})$ implies $\mathcal{R}(\mathbb{X}, \mathbb{Y}^\lambda, \mathbb{Z}) \subseteq \mathcal{R}(\mathbb{X}, \mathbb{Y}, \mathbb{Z})$; hence we also have $(r^\lambda, R^\lambda) \in \mathcal{R}(\mathbb{X}, \mathbb{Y}, \mathbb{Z})$. Then by the closure property of the achievable region we know $(R, r) \in \mathcal{R}(\mathbb{X}, \mathbb{Y}, \mathbb{Z})$. ■

Assume that (134) and (135) are true. If $\beta(\omega) := \frac{\rho_{XY}^2(\omega) - \rho_{XZ}^2(\omega)}{1 - \rho_{XY}^2(\omega)} > \mu$ then from (125),

$$\begin{aligned} & \inf_{0 \leq \omega < 2\pi} \{1 - \rho_{UX}^2(\omega)\} \\ &= \inf_{0 \leq \omega < 2\pi} \frac{\mu(1 - \rho_{XY}^2(\omega)(1 - \rho_{XZ}^2(\omega)))}{\rho_{XY}^2(\omega) - (1 + \mu)\rho_{XZ}^2(\omega) + \mu\rho_{XY}^2(\omega)\rho_{XZ}^2(\omega)} \end{aligned} \quad (138)$$

$$\geq \inf_{0 \leq \omega < 2\pi} \mu \frac{1 - \rho_{XY}^2(\omega)}{\rho_{XY}^2(\omega)} \quad (139)$$

$$> 0. \quad (140)$$

where (139) used the monotonically increasing property of the rational function on the right hand side of (138) in $\rho_{XZ}^2(\omega) \in [0, (1+\mu)\rho_{XY}^2(\omega) - \mu]$. This means that $\delta > 0$ in (133), which will be essential to applying Lemma 3.

For Wiener class Gaussian processes, the spectral function is continuous. Hence from (130), (131) and the definition of Riemann integral we have

$$\frac{1}{n} \sum_{i=1}^n \mathbb{E} \eta_i^{(n)} \rightarrow \frac{1}{4\pi} \int \log \left(\frac{1}{1 - \rho_{UX}^2(\omega)} \right) d\omega \quad (141)$$

$$= I(\mathbb{U}; \mathbb{X}). \quad (142)$$

Now fix $B > I(\mathbb{U}; \mathbb{X})$. Define $P_{\mathbf{U}|\mathbf{X}} := P_{\hat{\mathbf{U}}|\hat{\mathbf{X}}}$. According to Corollary 1, there exist non-degenerate linear transforms on \mathbf{U} and \mathbf{X} to obtain $\bar{\mathbf{U}}$ and $\bar{\mathbf{X}}$ such that $P_{\bar{\mathbf{U}}\bar{\mathbf{X}}} = \prod_{i=1}^n P_{\bar{U}_i\bar{X}_i}$. Let $\bar{\rho}_i^{(n)}$, $i = 1, \dots, n$ be the correlation coefficients between \bar{U}_i and \bar{X}_i . From the proof of Lemma 1 one can verify that $(\bar{\rho}_i^{(n)})^2$, $i = 1, \dots, n$ are eigenvalues of $\mathbf{I} - \Sigma_{\mathbf{X}}^{-\frac{1}{2}} \Sigma_{\mathbf{X}|\mathbf{U}} \Sigma_{\mathbf{X}}^{-\frac{1}{2}}$, and $(\rho_i^{(n)})^2$, $i = 1, \dots, n$ are eigenvalues of $\mathbf{I} - \Sigma_{\bar{\mathbf{X}}}^{-\frac{1}{2}} \Sigma_{\bar{\mathbf{X}}|\hat{\mathbf{U}}} \Sigma_{\bar{\mathbf{X}}}^{-\frac{1}{2}}$. However these two matrices are asymptotically equivalent, and their largest eigenvalues are uniformly upper bounded away from one, which follows immediately from Fact 5 and the following result.

Lemma 5. *Under the assumptions (134) and (135), we have*

(a)

$$\Sigma_{\mathbf{X}} \sim \Sigma_{\bar{\mathbf{X}}}, \quad \Sigma_{\mathbf{Y}} \sim \Sigma_{\bar{\mathbf{Y}}}, \quad \Sigma_{\mathbf{Z}} \sim \Sigma_{\bar{\mathbf{Z}}}. \quad (143)$$

Moreover, the smallest eigenvalues of these matrices are uniformly bounded (meaning that the bound is independent of n) away from zero, and their largest eigenvalues are also uniformly upper bounded.

(b)

$$\Sigma_{\mathbf{X}|\mathbf{U}} \sim \Sigma_{\bar{\mathbf{X}}|\hat{\mathbf{U}}}, \quad \Sigma_{\mathbf{Y}|\mathbf{U}} \sim \Sigma_{\bar{\mathbf{Y}}|\hat{\mathbf{U}}}, \quad \Sigma_{\mathbf{Z}|\mathbf{U}} \sim \Sigma_{\bar{\mathbf{Z}}|\hat{\mathbf{U}}}. \quad (144)$$

Moreover, the smallest eigenvalues of these matrices are uniformly bounded away from zero.

Proof: See Appendix G. ■

Therefore $\{(\bar{\rho}_i^{(n)})^2\}$ is asymptotically equally distributed as $\{(\rho_i^{(n)})^2\}$ on $[0, 1 - \delta_0]$ for some $\delta_0 > 0$ according to Fact 6. It follows that for any continuous function F on $[0, 1 - \delta_0]$,

$$\lim_{n \rightarrow \infty} \frac{1}{n} \sum_i F((\bar{\rho}_i^{(n)})^2) = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_i F((\rho_i^{(n)})^2). \quad (145)$$

Define $\bar{\eta}_i^{(n)} = \iota_{\bar{X}_i; \bar{U}_i}(\bar{X}_i; \bar{U}_i)$. Then fixing $\epsilon < \frac{B - I(\mathbb{U}; \mathbb{X})}{3 + I(\mathbb{U}; \mathbb{X})}$, there exists $t > 0$ such that for all n ,

$$\frac{1}{n} \ln \mathbb{P}(\iota_{\mathbf{X}; \mathbf{U}}(\mathbf{X}; \mathbf{U}) \geq nB) = \frac{1}{n} \ln \mathbb{P} \left(\frac{1}{n} \sum_{i=1}^n \bar{\eta}_i^{(n)} \geq B \right) \quad (146)$$

$$\leq \frac{1}{n} \sum_{i=1}^n \ln \mathbb{E} e^{t \bar{\eta}_i^{(n)}} - tB \quad (147)$$

$$\leq t(1 + \epsilon) \frac{1}{n} \sum_{i=1}^n \mathbb{E} \bar{\eta}_i^{(n)} + \epsilon t - tB \quad (148)$$

where (147) is from Markov's inequality (or the Chernoff bound) and (148) uses Lemma 3 and the fact that $|\bar{\rho}_i^{(n)}| < \sqrt{1 - \delta_0}$. Now let $F: x \mapsto \frac{1}{2} \log(\frac{1}{1-x})$. From (145) and (142), there exists $n_0 > 0$ such that for $n > n_0$,

$$\frac{1}{n} \sum_{i=1}^n \mathbb{E} \bar{\eta}_i^{(n)} < I(\mathbb{U}; \mathbb{X}) + \frac{\epsilon}{1 + \epsilon}. \quad (149)$$

Then (148) and (149) imply that for $n > n_0$,

$$\frac{1}{n} \ln \mathbb{P}(\iota_{\mathbf{X}; \mathbf{U}}(\mathbf{X}; \mathbf{U}) \geq nB) < t[(1 + \epsilon)I(\mathbb{U}; \mathbb{X}) + 2\epsilon - B] \quad (150)$$

$$< -t\epsilon. \quad (151)$$

To finish the achievability proof, we need to show that the bounds in Theorem 7 converge to zero for rate pairs in the interior of $\mathcal{R}(\mathbb{X}, \mathbb{Y}, \mathbb{Z})$. An inspection of the bounds in Theorem 7 reveals that it suffices to show (as $n \rightarrow \infty$)

- 1) $\mathbb{P}(\iota_{\mathbf{U}; \mathbf{X}}(\mathbf{U}; \mathbf{X}) > nB)$ converges to 0 exponentially fast;
- 2) $\mathbb{P}(\iota_{\mathbf{U}; \mathbf{Y}}(\mathbf{U}; \mathbf{Y}) < nC)$ converges to 0;
- 3) $\mathbb{P}(\iota_{\mathbf{U}; \mathbf{Z}}(\mathbf{U}; \mathbf{Z}) > nD)$ converges to 0 exponentially fast,

for $P_{\mathbf{U}\mathbf{X}\mathbf{Y}\mathbf{Z}} := P_{\hat{\mathbf{U}}|\hat{\mathbf{X}}} P_{\mathbf{X}\mathbf{Y}\mathbf{Z}}$, and any $B > I(\mathbb{U}; \mathbb{X})$, $C < I(\mathbb{U}; \mathbb{Y})$ and $D > I(\mathbb{U}; \mathbb{Z})$. Speed of converge is imposed in 1) and 3), so that upon choosing δ to be exponentially decreasing in n , the term

$$T^* + 8\delta = 4(T_1 + T_2 + 3T_3 + 2\delta) \quad (152)$$

in (64) is also exponentially decreasing in n , thus annihilating the term $\log \frac{M^{\frac{3}{2}}}{\delta}$ in (64), which grows linearly in n . From (151) we see the validity of property 1).

The proof of 3) follows the same steps as that of 1). Similar to (142), we have

$$\frac{1}{n} I(\hat{\mathbf{U}}; \hat{\mathbf{Z}}) = \frac{1}{n} I(\hat{\mathbf{U}}; \hat{\mathbf{Z}}) \quad (153)$$

$$\rightarrow \frac{1}{4\pi} \int \log \left(\frac{1}{1 - \rho_{XU}^2(\omega) \rho_{XZ}^2(\omega)} \right) d\omega \quad (154)$$

$$= I(\mathbb{U}; \mathbb{Z}). \quad (155)$$

And as in (146)-(148), fixing $\epsilon < \frac{D - I(\mathbb{U}; \mathbb{Z})}{3 + I(\mathbb{U}; \mathbb{Z})}$ there exists $t > 0$ so that we can upper bound

$$\frac{1}{n} \ln \mathbb{P}(\iota_{\mathbf{Z}; \mathbf{U}}(\mathbf{Z}; \mathbf{U}) \geq nD) \leq t(1 + \epsilon) \frac{1}{n} I(\mathbb{U}; \mathbb{Z}) + \epsilon t - tD. \quad (156)$$

Then (155) and (156) will imply 3) once

$$\lim_{n \rightarrow \infty} \frac{1}{n} [I(\mathbb{U}; \mathbb{Z}) - I(\hat{\mathbf{U}}; \hat{\mathbf{Z}})] = 0 \quad (157)$$

is established. Now suppose $\mathbf{U} \rightarrow \bar{\mathbf{U}}$ and $\mathbf{Z} \rightarrow \bar{\mathbf{Z}}$ are the diagonalizing linear transforms in Lemma 1. Then it suffices to show that $\{\rho_{\bar{U}_i; \bar{Z}_i}^2\}_{i=1}^n$ and $\{\rho_{\bar{U}_i; \hat{Z}_i}^2\}_{i=1}^n$ are asymptotically equally distributed on $[0, 1 - \delta_0]$. Indeed, we first note that $\max_{1 \leq i \leq n} |\rho_{\bar{U}_i; \bar{Z}_i}|$ is the maximal correlation coefficient between $\bar{\mathbf{U}}$ and $\bar{\mathbf{Z}}$, and $\max_{1 \leq i \leq n} \rho_{\bar{U}_i; \bar{X}_i}$ is the maximal correlation coefficient between $\bar{\mathbf{U}}$ and $\bar{\mathbf{X}}$, hence $\max_{1 \leq i \leq n} |\rho_{\bar{U}_i; \bar{Z}_i}| \leq \max_{1 \leq i \leq n} \rho_{\bar{U}_i; \bar{X}_i} \leq \sqrt{1 - \delta_0}$ due to the Markov chain $\bar{\mathbf{U}} - \bar{\mathbf{X}} - \bar{\mathbf{Z}}$. By a similar argument we also have $\max_{1 \leq i \leq n} |\rho_{\hat{U}_i; \hat{Z}_i}| \leq \sqrt{1 - \delta_0}$. Hence we have shown

that $\rho_{\underline{U}_i; \underline{Z}_i}^2$ and $\rho_{\underline{U}_i; \underline{Z}_i}^2$ are bounded in $[0, 1 - \delta_0]$. To show their asymptotic equidistribution, it remains to prove that

$$\mathbf{I} - \Sigma_{\mathbf{Z}}^{-\frac{1}{2}} \Sigma_{\mathbf{Z}|\mathbf{U}} \Sigma_{\mathbf{Z}}^{-\frac{1}{2}} \sim \mathbf{I} - \Sigma_{\underline{\mathbf{Z}}}^{-\frac{1}{2}} \Sigma_{\underline{\mathbf{Z}}|\underline{\mathbf{U}}} \Sigma_{\underline{\mathbf{Z}}}^{-\frac{1}{2}} \quad (158)$$

which follows immediately from Lemma 5 and Fact 5.

The proof of 2) is simpler: without an requirement on the speed of convergence, we can just use a coarse upper bounded via Chebyshev's inequality:

$$\mathbb{P}(\iota_{\mathbf{U}; \mathbf{Y}}(\mathbf{U}; \mathbf{Y}) < nC) \leq \frac{\text{Var}(\iota_{\mathbf{U}; \mathbf{Y}}(\mathbf{U}; \mathbf{Y}))}{n^2(\frac{1}{n}I(\mathbf{U}; \mathbf{Y}) - C)^2} \quad (159)$$

The roles of \mathbf{Y} and \mathbf{Z} are identical to the counterparts of (155) and (157) hold, so we have

$$\lim_{n \rightarrow \infty} \frac{1}{n} I(\mathbf{U}; \mathbf{Y}) = I(\underline{\mathbf{U}}; \underline{\mathbf{Y}}). \quad (160)$$

Suppose $\mathbf{U} \rightarrow \underline{\mathbf{U}}$ and $\mathbf{Z} \rightarrow \underline{\mathbf{Z}}$ are the diagonalizing linear transforms in Lemma 1. Then as before $\max_{1 \leq i \leq n} \rho_{\underline{U}_i; \underline{Y}_i}^2 \leq 1 - \delta_0$ which is uniformly upper bounded for all n . Hence there exists a uniform upper bound $\text{Var}(\iota_{\underline{U}_i; \underline{Y}_i}(\underline{U}_i; \underline{Y}_i)) < V$ for some $V > 0$ independent of n . Then $\text{Var}(\iota_{\mathbf{U}; \mathbf{Y}}(\mathbf{U}; \mathbf{Y})) \leq nV$, and so condition 2) is true by virtue of (159) and (160). The achievability proof for Theorem 6 is completed.

Remark 11. Although the assumption that $\beta(\omega)$ is well defined for each $\omega \in [0, 2\pi)$ in Theorem 6 is fairly reasonable, it is still possible that $\beta(\omega)$ is *not* defined for a set of frequencies of measure zero yet the Lebesgue integrals in (58) and (59) still make sense. In such a case, we no longer have the convenient conditions in (134). However, if only the first two conditions in (134) are unfulfilled and $\min_{0 \leq \omega < 2\pi} S_Z(\omega) > 0$ remains true, we can still prove Theorem 6 by showing the achievability for some degraded \mathbb{X} and \mathbb{Y} first and then applying the closure property of the achievable region, which is similar to the argument in Lemma 4. Nonetheless, our proof cannot be easily extended to the case where $\min_{0 \leq \omega < 2\pi} S_Z(\omega) = 0$, since degrading the eavesdropper's observation can only augment the achievable region.

VI. DISCUSSION

As remarked earlier, Theorem 3 is analogous to a rate distortion theorem for product sources under additive distortion measure; in fact one can show a similar result for channel capacity with additive cost constraints. Related phenomena in information theory also include the additivity of channel capacity (without input constraints) and Wyner's common information [27]. In those cases, the achievable rate region of the product source/channel is the Minkowski sum of the achievable region of the factor sources/channels. The evidence points to the principle that rate splitting is optimal for product resources asymptotically in most information theoretic problems admitting single-letter solutions.⁸ Indeed, the algebraic manipulations in the converse proofs usually rely only on the independence of $\{X_t\}$, and do not require them to be

⁸Exceptions to this principle do exist, for example the key generation with an omniscient helper problem [28], the mismatched broadcast channel with a common message [19, Remark 9.6], and lossy compression with mismatched side-information [29].

identically distributed. Hence the main element in proving such a result about rate splitting (e.g. Lemma 6 in the appendix) is usually related to the converse proof of the corresponding coding theorem. However, there are a number of examples where the *achievable* regions fail to satisfy such an additive property (c.f. a relay broadcast channel discussed in [30, Remark 17]), although the *exact* region is not known. Moreover, this rule also fails quite often for coding problems of combinatorial nature. For example, the additivity of zero error capacity was a famous conjecture [5][31] which has now been disproved [32].

It is also interesting to consider the constant

$$s_*(X; Y) := \inf_{U-X-Y, I(U; X) \neq 0} \frac{I(U; Y)}{I(U; X)} = \inf_{Q_X \neq P_X} \frac{D(Q_Y || P_Y)}{D(Q_X || P_X)} \quad (161)$$

where $Q_X \rightarrow P_{Y|X} \rightarrow Q_Y$. Interestingly, $s_*(X; Y)$ does not tensorize, and in fact it usually vanishes exponentially in L for i.i.d. $(X_i, Y_i)_{i=1}^L$. Indeed if $H(X|Y) > 0$, we can choose $R \in (I(X; Y), H(X))$. Set $P_{Y^L|X^L} = \prod_{i=1}^L P_{Y_i|X_i}$ and $P_{X^L} = \prod_{i=1}^L P_{X_i}$. By resolvability/soft covering lemma and its strong converse [27][33][24], we can choose a $[2^{nR}]$ -type⁹ distribution Q_{X^L} and set $Q_{X^L} \rightarrow P_{Y^L|X^L} \rightarrow Q_{Y^L}$ such that $D(Q_{Y^L} || P_{Y^L})$ converges to zero exponentially as $n \rightarrow \infty$ whereas $D(Q_{X^L} || P_{X^L})$ is bounded away from zero, from which the exponential decay of $\frac{D(Q_{Y^L} || P_{Y^L})}{D(Q_{X^L} || P_{X^L})}$ follows. This implies, among other things, that no information theoretic problem can have a single-letter solution of the form $[I(U; Y), \infty) \times [0, I(U; X)]$.

VII. ACKNOWLEDGMENTS

We are pleased to acknowledge Sanket Satpathy for suggesting the Minkowski sum interpretation in Theorem 3, and Shun Watanabe for pointing out the last two examples in footnote 8. This work was supported by NSF under Grants CCF-1350595, CCF-1116013, CCF-1319299, CCF-1319304, and the Air Force Office of Scientific Research under Grant FA9550-15-1-0180, FA9550-12-1-0196.

APPENDIX A

A KEY OBSERVATION FOR PRODUCT SOURCES

The following observation is central to the proof of both tensorization property of $s_Z^*(X; Y)$ and the optimality of rate splitting in Theorem 3. It thus manifests how the two problems are inherently connected.

Lemma 6. Suppose that $\{(X_i, Y_i, Z_i)\}_{i=1}^L$ possess the product structure of 1 and (2), and (U, V) are r.v.'s such that $(U, V) - X^L - (Y^L, Z^L)$. Then there exist U^L and V^L such

⁹In [33] a probability distribution P is called M -type if $P(a)M$ is an integer for each $a \in \mathcal{A}$.

that $(U_i, V_i) - X_i - (Y_i, Z_i)$ for $i = 1, \dots, L$ and

$$I(U, V; X^L) - I(U, V; Y^L) \geq \sum_{i=1}^L [I(U_i, V_i; X_i) - I(U_i, V_i; Y_i)], \quad (162)$$

$$I(V; Y^L|U) - I(V; Z^L|U) = \sum_{i=1}^L [I(V_i; Y_i|U_i) - I(V_i; Z_i|U_i)]. \quad (163)$$

Proof: Suppose we are given the additional condition that $Y^L - X^L - Z^L$ form a Markov chain, then (1) and (2) will imply $P_{X^L Y^L Z^L} = \prod_{i=1}^L P_{X_i, Y_i, Z_i}$ which will facilitate the proof. Now in general $Y^L - X^L - Z^L$ may not be true; but notice that the expressions in (162) and (163) depend only on the marginal distributions of Y^L and Z^L given X^L , rather than how they are correlated given X^L . Hence we can convert the source distribution to a new one where $Y^L - X^L - Z^L$ while the conditional marginal distributions of (X^L, Y^L) and (X^L, Z^L) remain the same.

To carry out the above procedure, choose \bar{Z}^L such that

$$\begin{aligned} P_{UVX^LY^LZ^L}(u, v, x^L, y^L, z^L) \\ = P_{UVX^L}(u, v, x^L) P_{Y^L|X^L}(y^L|x^L) P_{Z^L|X^L}(z^L|x^L). \end{aligned} \quad (164)$$

Define $\bar{U}_i = (Y^{i-1}, \bar{Z}_{i+1}^L, U)$ and $V_i = V$. Then $(\bar{U}_i, V_i) - X_i - (Y_i, \bar{Z}_i)$ for each i . Moreover

$$I(V; Y^L|U) - I(V; \bar{Z}^L|U) = \sum_{i=1}^L [I(V_i; Y_i|\bar{U}_i) - I(V_i; \bar{Z}_i|\bar{U}_i)] \quad (165)$$

holds, which is a standard identity in multiuser information theory (see for example [34, Lemma 4.1]),

Next, observe that

$$\begin{aligned} I(U, V; X^L) - I(U, V; Y^L) \\ = \sum_{i=1}^L [I(U, V; X_i|X_{i+1}^L, Y^{i-1}) - I(U, V; Y_i|X_{i+1}^L, Y^{i-1})] \end{aligned} \quad (166)$$

$$= \sum_{i=1}^L [I(U, V, X_{i+1}^L, Y^{i-1}; X_i) - I(U, V, X_{i+1}^L, Y^{i-1}; Y_i)] \quad (167)$$

$$= \sum_{i=1}^L [I(U, V, X_{i+1}^L, Y^{i-1}, \bar{Z}_{i+1}^L; X_i) - I(U, V, X_{i+1}^L, Y^{i-1}, \bar{Z}_{i+1}^L; Y_i)] \quad (168)$$

$$\begin{aligned} = \sum_{i=1}^L [I(U, V, Y^{i-1}, \bar{Z}_{i+1}^L; X_i) - I(U, V, Y^{i-1}, \bar{Z}_{i+1}^L; Y_i)] \\ + \sum_{i=1}^L [I(X_{i+1}^L; X_i|U, V, Y^{i-1}, \bar{Z}_{i+1}^L) - I(X_{i+1}^L; Y_i|U, V, Y^{i-1}, \bar{Z}_{i+1}^L)] \end{aligned} \quad (169)$$

$$\geq \sum_{i=1}^L [I(U, V, Y^{i-1}, \bar{Z}_{i+1}^L; X_i) - I(U, V, Y^{i-1}, \bar{Z}_{i+1}^L; Y_i)] \quad (170)$$

$$= \sum_{i=1}^L [I(\bar{U}_i, V_i; X_i) - I(\bar{U}_i, V_i; Y_i)], \quad (171)$$

where (166) is again an application of [34, Lemma 4.1], and (167) is from the independence $(X_i, Y_i) \perp (X_{i+1}^L, Y^{i-1})$. Equality (168) follows from the Markov condition $\bar{Z}_{i+1}^L - (U, V, X_{i+1}^L, Y^{i-1}) - (X_i, Y_i)$. Inequality (170) is because of $I(X_{i+1}^L; X_i|U, V, Y^{i-1}, \bar{Z}_{i+1}^L) = I(X_{i+1}^L; X_i, Y_i|U, V, Y^{i-1}, \bar{Z}_{i+1}^L)$, due to the Markov condition $X_{i+1}^L - (U, V, Y^{i-1}, \bar{Z}_{i+1}^L, X_i) - Y_i$.

Finally, for each i let U_i be a r.v. such that

$$P_{U_i|V_i X_i Y_i Z_i}(u_i|v_i, x_i, y_i, z_i) = P_{\bar{U}_i|V_i X_i}(u_i|v_i, x_i). \quad (172)$$

Then (U_i, V_i, X_i, Z_i) and $(\bar{U}_i, V_i, X_i, \bar{Z}_i)$ have the same distribution, hence

$$I(V_i; Z_i|U_i) = I(V_i; \bar{Z}_i|\bar{U}_i). \quad (173)$$

By the same token, we also have

$$I(V_i; Y_i|U_i) = I(V_i; Y_i|\bar{U}_i), \quad (174)$$

$$I(U_i, V_i; Y_i) = I(\bar{U}_i, V_i; Y_i), \quad (175)$$

$$I(U_i, V_i; X_i) = I(\bar{U}_i, V_i; X_i), \quad (176)$$

$$I(V; Z^L|U) = I(V; \bar{Z}^L|U). \quad (177)$$

Therefore we see that (165), (171) imply the desired result, once we make the substitutions with (173)-(177). ■

In the case where Z^L does not exist, the tensorization property of $s^*(X; Y)$ and Theorem 3 can also be proved using the following result.

Lemma 7. Suppose that $\{(X_i, Y_i)\}_{i=1}^L$ possess the product structure of (1) and (2), and U is a r.v. such that $U - X^L - Y^L$.

Then there exist U^L such that $U_i - X_i - Y_i$ for $i = 1, \dots, L$ and

$$I(U; X^L) = \sum_{i=1}^L I(U_i; X_i), \quad (178)$$

$$I(U; Y^L) \leq \sum_{i=1}^L I(U_i; Y_i). \quad (179)$$

Proof: By induction, it suffices to prove the case of $L = 2$. Let $U_1 := U$ and $U_2 := (U, X_1)$. We have:

$$\begin{aligned} I(U; X^2) &= I(U; X_1) + I(U; X_2|X_1) \\ &= I(U; X_1) + [I(U; X_2|X_1) + I(X_1; X_2)] \\ &= I(U; X_1) + I(U, X_1; X_2), \end{aligned}$$

$$\begin{aligned} I(U; Y^2) &= I(U; Y_1) + I(U; Y_2|Y_1) \\ &= I(U; Y_1) + [I(U; Y_2|Y_1) + I(Y_1; Y_2)] \\ &= I(U; Y_1) + I(U, Y_1; Y_2) \\ &\leq I(U; Y_1) + I(U, X_1, Y_1; Y_2) \\ &= I(U; Y_1) + I(U, X_1; Y_2). \end{aligned} \quad (180)$$

where the last equality is from the Markov chain $Y_1 - (U, X_1) - Y_2$. ■

Note that setting Z^L in Lemma 6 to be a constant will imply the existence of U^L satisfying $U_i - X_i - Y_i$ and the inequalities

$$I(U; X^L) \geq \sum_{i=1}^L I(U_i; X_i), \quad (181)$$

$$I(U; Y^L) = \sum_{i=1}^L I(U_i; Y_i), \quad (182)$$

which are different from (178) and (179). Hence Lemma 7 is not a special case of Lemma 6.

APPENDIX B PROOF OF THEOREM 4

- 1) From the data processing inequality the denominator in (39) is nonnegative, and $s_Z^*(X; Y) \leq 1$. If there exists U such that $I(U; X) - I(U; Y) > 0$, we can choose V independent of U, X, Y so that the numerator vanishes whereas the denominator is positive, which shows that $s_Z^*(X; Y) \geq 0$. Otherwise if $I(U; X) - I(U; Y) = 0$ for all U , the numerator will always be nonnegative:

$$\begin{aligned} &I(V; Y|U) - I(V; Z|U) \\ &= I(U, V; Y) - I(U, V; Z) - I(U; Y) + I(U; Z) \\ &= I(U, V; X) - I(U, V; Z) - I(U; X) + I(U; Z). \end{aligned} \quad (183)$$

Hence $s_Z^*(X; Y) \geq 0$ always holds.

Of course, from an operational viewpoint $0 \leq s_Z^*(X; Y) \leq 1$ must be true because of Part 3) as well.

- 2) We only show that

$$s_Z^*(X^L; Y^L) \leq \max_{1 \leq i \leq n} s_{Z_i}^*(X_i; Y_i) \quad (184)$$

since the other direction is trivial. For any U, V such that $(U, V) - X^L - (Y^L, Z^L)$ and both

$$I(U, V; X^L) - I(U, V; Y^L) > 0 \quad (185)$$

and

$$I(V; Y^L|U) - I(V; Z^L|U) > 0, \quad (186)$$

let U^L, V^L be as in Lemma 6 in the appendix. That is, U^L, V^L are such that $(U_i, V_i) - X_i - (Y_i, Z_i)$ for each i and both

$$I(U, V; X^L) - I(U, V; Y^L) \geq \sum_{i=1}^L [I(U_i, V_i; X_i) - I(U_i, V_i; Y_i)] \quad (187)$$

and

$$I(V; Y^L|U) - I(V; Z^L|U) = \sum_{i=1}^L [I(V_i; Y_i|U_i) - I(V_i; Z_i|U_i)] \quad (188)$$

hold. Then

$$\begin{aligned} &\frac{I(V; Y^L|U) - I(V; Z^L|U)}{I(U, V; X^L) - I(U, V; Y^L)} \\ &\leq \frac{\sum_{i=1}^L [I(V_i; Y_i|U_i) - I(V_i; Z_i|U_i)]}{\sum_{i=1}^L [I(U_i, V_i; X_i) - I(U_i, V_i; Y_i)]} \end{aligned} \quad (189)$$

$$\begin{aligned} &\leq \max_{i \in \mathcal{I}} \frac{I(V_i; Y_i|U_i) - I(V_i; Z_i|U_i)}{I(U_i, V_i; X_i) - I(U_i, V_i; Y_i)} \\ &\leq \max_{1 \leq i \leq L} \sup_{U_i, V_i} \frac{I(V_i; Y_i|U_i) - I(V_i; Z_i|U_i)}{I(U_i, V_i; X_i) - I(U_i, V_i; Y_i)} \end{aligned} \quad (190)$$

where \mathcal{I} is the set of indices such that $I(U_i, V_i; X_i) - I(U_i, V_i; Y_i) \neq 0$, and the suprema are over all U_i, V_i such that $(U_i, V_i) - X_i - (Y_i, Z_i)$ and $I(U_i, V_i; X_i) - I(U_i, V_i; Y_i) \neq 0$. Supremizing with respect to U, V on the left hand side of (189) shows the tensorization property of $\frac{s_Z^*(X; Y)}{1 - s_Z^*(X; Y)}$, which is equivalent to the tensorization property of $s_Z^*(X; Y)$.

- 3) One direction of the inequality is trivial: if U and V are such that $I(V; Y|U) - I(V; Z|U) \geq 0$, we have (see (191)-(193)) For the other direction, to construct a distribution on (U, V, X, Y, Z) from Q , we use a binary U biased heavily toward zero. When $U = 1$, the distribution is as specified by Q . When $U = 0$, V is independent of (X, Y, Z) , and the marginal distribution on X balanced slightly to counteract Q , so that on average the distribution on X is the source distribution. Even though this distribution is only rarely behaving according to Q (i.e. only when $U = 1$, which has low probability), we will see that the quantity of interest only depends on Q . Formally, for any Q_{VX} , consider

$$Q_{VX}^{(1)} := Q_{VX}, \quad (194)$$

$$Q_{VX}^{(0)} := P_V \cdot \frac{P_X - \alpha Q_X^{(1)}}{1 - \alpha}, \quad (195)$$

$$\begin{aligned} P_{XUV}^\alpha(x, u, v) &:= (1 - \alpha) Q_{VX}^{(0)}(v, x) 1_{u=0} \\ &\quad + \alpha Q_{VX}^{(1)}(v, x) 1_{u=1}, \end{aligned} \quad (196)$$

where P_V is an arbitrary probability distribution on \mathcal{V} . Then clearly $P_X^\alpha = P_X$ for each $0 < \alpha < 1$. Finally, define

$$P_{XYZUV}^\alpha := P_{XUV}^\alpha P_{YZ|X}. \quad (197)$$

In (43) we have implicitly assumed that $D(Q_X||P_X)$ is well defined and so the support of Q_X is a subset of the support of P_X . Thus (195) is a well-defined distribution for $\alpha > 0$ small enough. Then, we can verify that $P_{XYZ}^\alpha = P_{XYZ}$ and the Markov chain $(U, V) - X - (Y, Z)$ with respect to P^α . Next observe that (see (198)-(200)) as $\alpha \downarrow 0$, where (U, V, X, Y, Z) has the joint distribution $P_{UVXYZ} := P_{UVXYZ}^\alpha$, and the distribution of $(\bar{V}, \bar{X}, \bar{Y}, \bar{Z})$ is as in (44). Equation (198) is from the independence between V and (X, Y, Z) under $U = 0$. To justify (200), recall the property of relative entropy that if $P_\lambda := \lambda P_1 + (1 - \lambda)P_0$ is a distribution for sufficiently small $\lambda > 0$, then $D(P_\lambda||P_0) = o(\lambda)$. This smoothness condition implies that

$$D(P_{X|U=0}||P_X) = o(\alpha), \quad (201)$$

$$D(P_{Y|U=0}||P_Y) = o(\alpha). \quad (202)$$

Therefore (200) is true, and the \geq part of (43) holds.

- 4) In the case of degraded sources $X - Y - Z$, we can write (see (203)-(206)) where the first inequality is from $-D(P_{\bar{Y}}||P_Y) + D(P_{\bar{Z}}||P_Z) \leq 0$, and the second inequality used the fact that $D(P_{Y|\bar{V}=v}||P_Y) - D(P_{Z|\bar{V}=v}||P_Z) \geq 0$. This establishes the “ \leq ” part of (45). Conversely, for any Q_X , define

$$Q_X^{(1)} = Q_X, \quad (207)$$

$$Q_X^{(0)} = \frac{P_X - \alpha Q_X^{(1)}}{1 - \alpha}, \quad (208)$$

$$Q_{VX}^\alpha(v, x) = \alpha Q_{VX}^{(1)}(v, x)1_{v=1} + (1 - \alpha)Q_{VX}^{(0)}(v, x)1_{v=0}. \quad (209)$$

Let $P_{\bar{V}\bar{X}\bar{Y}\bar{Z}} = Q_{VX}^\alpha P_{YZ|X}$. Notice that $P_{\bar{X}\bar{Y}\bar{Z}} =$

P_{XYZ} . Then

$$\lim_{\alpha \downarrow 0} \frac{I(\bar{V}; \bar{Y}) - I(\bar{V}; \bar{Z})}{I(\bar{V}; \bar{X}) - I(\bar{V}; \bar{Z}) + D(Q_X^\alpha||P_X) - D(Q_Y^\alpha||P_Y)} \quad (210)$$

$$= \lim_{\alpha \downarrow 0} \frac{I(\bar{V}; \bar{Y}) - I(\bar{V}; \bar{Z})}{I(\bar{V}; \bar{X}) - I(\bar{V}; \bar{Z})} \quad (211)$$

$$= \frac{D(Q_Y||P_Y) - D(Q_Z||P_Z)}{D(Q_X||P_X) - D(Q_Z||P_Z)} \quad (212)$$

This implies that

$$\sup_{R_{VX}} \frac{I(\bar{V}; \bar{Y}) - I(\bar{V}; \bar{Z})}{I(\bar{V}; \bar{X}) - I(\bar{V}; \bar{Z}) + D(R_X||P_X) - D(R_Y||P_Y)} \geq \frac{D(Q_Y||P_Y) - D(Q_Z||P_Z)}{D(Q_X||P_X) - D(Q_Z||P_Z)} \quad (213)$$

where $P_{\bar{V}\bar{X}\bar{Y}\bar{Z}}(v, x, y, z) = R_{VX}(v, x)P_{YZ|X}(y, z|x)$. The proof of (45) is complete since Q_X in the right side of (213) is arbitrary.

- 5) If the sources are of the form $X = (X', Z)$, $Y = (Y', Z)$, we have

$$\begin{aligned} & \frac{D(Q_Y||P_Y) - D(Q_Z||P_Z)}{D(Q_X||P_X) - D(Q_Z||P_Z)} \\ &= \frac{\int D(Q_{Y'|Z=z}||P_{Y'|Z=z})dQ_Z(z)}{\int D(Q_{X'|Z=z}||P_{X'|Z=z})dQ_Z(z)} \\ &\leq \text{ess sup}_{z \in \mathcal{Z}} \sup_{Q_{X'}} \frac{D(Q_{Y'|Z=z}||P_{Y'|Z=z})}{D(Q_{X'|Z=z}||P_{X'|Z=z})}, \end{aligned} \quad (214)$$

where in the last supremum $Q_{X'Y'} = Q_{X'}P_{Y'|X'Z=z}$. Conversely for any $z_0 \in \mathcal{Z}$ and $Q_{X'}$ in (214), define

$$\begin{aligned} \tilde{Q}_X(x) &= \tilde{Q}_{X'Z}(x', z) \\ &= P_Z(z_0)Q_{X'}(x')1_{z=z_0} \end{aligned} \quad (215)$$

$$+ P_Z(z)P_{X'|Z=z}(x')1_{z \neq z_0}. \quad (216)$$

Then

$$\frac{D(\tilde{Q}_Y||P_Y) - D(\tilde{Q}_Z||P_Z)}{D(\tilde{Q}_X||P_X) - D(\tilde{Q}_Z||P_Z)} = \frac{D(Q_{Y'}||P_{Y'|Z=z_0})}{D(Q_{X'}||P_{X'|Z=z_0})}. \quad (217)$$

This establishes (46).

- 6) When Z is constant, we recover $s^*(X; Y) = \sup_{Q_U \neq P_U} \frac{I(U; Y)}{I(U; X)}$ by either (45) or (46).

$$\begin{aligned} & \frac{I(V; Y|U) - I(V; Z|U)}{I(V; X|U) - I(V; Z|U) + I(U; X) - I(U; Y)} \\ &= \frac{\int [I(V; Y|U=u) - I(V; Z|U=u)]dP_U(u)}{\int [I(V; X|U=u) - I(V; Z|U=u) + D(P_{X|U=u}||P_X) - D(P_{Y|U=u}||P_Y)]dP_U(u)} \end{aligned} \quad (191)$$

$$\leq \sup_u \frac{I(V; Y|U=u) - I(V; Z|U=u)}{I(V; X|U=u) - I(V; Z|U=u) + D(P_{X|U=u}||P_X) - D(P_{Y|U=u}||P_Y)} \quad (192)$$

$$\leq \sup_{Q_{VX}} \frac{I(\bar{V}; \bar{Y}) - I(\bar{V}; \bar{Z})}{I(\bar{V}; \bar{X}) - I(\bar{V}; \bar{Z}) + D(Q_X||P_X) - D(Q_Y||P_Y)}. \quad (193)$$

APPENDIX C
PROOF OF LEMMA 1

With the invertible linear transform $\tilde{\mathbf{X}} := \Sigma_{\mathbf{X}}^{-1/2} \mathbf{X}$, we have

$$\Sigma_{\tilde{\mathbf{X}}} = \begin{pmatrix} \mathbf{I}_{r_x} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}, \quad (218)$$

where $r_x = \text{rank}(\Sigma_{\mathbf{X}})$. Similar structures are also present in $\Sigma_{\tilde{\mathbf{Y}}}$ and $\Sigma_{\tilde{\mathbf{Z}}}$. By positive-semidefiniteness of the covariance matrix, we have the form

$$\begin{aligned} \Sigma_{\tilde{\mathbf{X}}, \tilde{\mathbf{Y}}} &= \begin{pmatrix} \mathbf{A}_{x,y} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}, \\ \Sigma_{\tilde{\mathbf{X}}, \tilde{\mathbf{Z}}} &= \begin{pmatrix} \mathbf{A}_{x,z} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}, \end{aligned} \quad (219)$$

where $\mathbf{A}_{x,y}$ and $\mathbf{A}_{x,z}$ are $r_x \times r_y$ and $r_x \times r_z$ matrices, respectively. However, we also have

$$\Sigma_{\tilde{\mathbf{X}}, \tilde{\mathbf{Y}}} = \Sigma_{\mathbf{X}}^{-1/2} \Sigma_{\mathbf{X}, \mathbf{Y}} \Sigma_{\mathbf{Y}}^{-1/2}, \quad (220)$$

$$\Sigma_{\tilde{\mathbf{X}}, \tilde{\mathbf{Z}}} = \Sigma_{\mathbf{X}}^{-1/2} \Sigma_{\mathbf{X}, \mathbf{Z}} \Sigma_{\mathbf{Z}}^{-1/2}, \quad (221)$$

Hence if \mathbf{G} and \mathbf{H} as defined in (33) and (34) commute, then so do $\mathbf{A}_{x,y} \mathbf{A}_{y,x}$ and $\mathbf{A}_{x,z} \mathbf{A}_{z,x}$. Since commuting matrices are simultaneously diagonalizable [35], that is, there exists an orthogonal matrix \mathbf{Q}_x such that $\mathbf{Q}_x \mathbf{A}_{x,y} \mathbf{A}_{y,x} \mathbf{Q}_x^\top$ and $\mathbf{Q}_x \mathbf{A}_{x,z} \mathbf{A}_{z,x} \mathbf{Q}_x^\top$ are diagonal. This in turn implies the existence of \mathbf{Q}_y and \mathbf{Q}_z such that $\mathbf{Q}_y \mathbf{A}_{y,x} \mathbf{Q}_y^\top$ and $\mathbf{Q}_z \mathbf{A}_{z,x} \mathbf{Q}_z^\top$ are diagonal. Therefore, after the transforms

$$\mathbf{X} \mapsto \bar{\mathbf{X}} := \begin{pmatrix} \mathbf{Q}_x & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{n-r_x} \end{pmatrix} \Sigma_{\mathbf{X}}^{-1/2} \mathbf{X}, \quad (222)$$

$$\mathbf{Y} \mapsto \bar{\mathbf{Y}} := \begin{pmatrix} \mathbf{Q}_y & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{n-r_y} \end{pmatrix} \Sigma_{\mathbf{Y}}^{-1/2} \mathbf{Y}, \quad (223)$$

$$\mathbf{Z} \mapsto \bar{\mathbf{Z}} := \begin{pmatrix} \mathbf{Q}_z & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{n-r_z} \end{pmatrix} \Sigma_{\mathbf{Z}}^{-1/2} \mathbf{Z}, \quad (224)$$

$$(225)$$

the matrices $\Sigma_{\tilde{\mathbf{X}}}$, $\Sigma_{\tilde{\mathbf{Y}}}$, $\Sigma_{\tilde{\mathbf{Z}}}$, $\Sigma_{\tilde{\mathbf{X}}\tilde{\mathbf{Y}}}$ and $\Sigma_{\tilde{\mathbf{X}}\tilde{\mathbf{Z}}}$ are diagonal.

Conversely, if the asserted linear transforms exist, then there must exist orthogonal matrices \mathbf{Q}_y and \mathbf{Q}_z such that $\mathbf{Q}_y \mathbf{A}_{y,x} \mathbf{Q}_y^\top$ and $\mathbf{Q}_z \mathbf{A}_{z,x} \mathbf{Q}_z^\top$ are diagonal. Hence $\mathbf{A}_{x,y} \mathbf{A}_{y,x}$ and $\mathbf{A}_{x,z} \mathbf{A}_{z,x}$ commute, and so do \mathbf{G} and \mathbf{H} .

APPENDIX D
CONNECTION BETWEEN GAUSSIAN AND BERNOULLI
SOURCES IN EXAMPLE 2

Suppose $P_{\mathbf{U}\mathbf{V}\mathbf{W}} = \prod_{i=1}^L P_{U_i V_i W_i}$, and U_i, V_i and W_i are symmetric Bernoulli random variable such that

$$1 - 2\mathbb{P}[U_i \neq V_i] = \rho_{XY}, \quad 1 - 2\mathbb{P}[U_i \neq W_i] = \rho_{XZ}. \quad (226)$$

Define

$$\bar{X}_L := \frac{1}{L} \sum_{i=1}^L U_i, \quad \bar{Y}_L := \frac{1}{L} \sum_{i=1}^L V_i, \quad \bar{Z}_L := \frac{1}{L} \sum_{i=1}^L W_i, \quad (227)$$

where the additions are on \mathbb{R} . Assuming without loss of generality that X, Y and Z have unit variances, then by central limit theorem $P_{\bar{X}_L \bar{Y}_L}$ and $P_{\bar{X}_L \bar{Z}_L}$ converge to P_{XY} and P_{XZ} as $L \rightarrow \infty$, hence we expect (without a formal proof here) that $\eta_Z(X; Y) = \lim_{L \rightarrow \infty} \eta_{\bar{Z}_L}(\bar{X}_L; \bar{Y}_L)$. Observe that

$$\eta_{\bar{Z}_L}(\bar{X}_L; \bar{Y}_L) = \eta_{\mathbf{W}}(\bar{X}_L; \bar{Y}_L) \quad (228)$$

$$\leq \eta_{\mathbf{W}}(\mathbf{U}; \mathbf{V}) \quad (229)$$

$$= \eta_{W_1}(U_1; V_1) \quad (230)$$

where (228) is because \bar{Z}_L is a sufficient statistic of \mathbf{W} for (\bar{X}_L, \bar{Y}_L) ; (229) is because processing \mathbf{U} and \mathbf{V} reduces key capacity; and (230) uses the tensorization property (42). Then from (47) we see $\eta_Z(X; Y) \leq \frac{\rho_{XY}^2 - \rho_{XZ}^2}{1 - \rho_{XZ}^2}$. Note that this central limit argument is similar to a celebrated proof of Gaussian hypercontractivity using Boolean hypercontractivity

$$\begin{aligned} & \frac{I(V; Y|U) - I(V; Z|U)}{I(V; X|U) - I(V; Z|U) + I(U; X) - I(U; Y)} \\ &= \frac{\alpha[I(V; Y|U=1) - I(V; Z|U=1)]}{\alpha[I(V; X|U=1) - I(V; Z|U=1)] + I(U; X) - I(U; Y)} \end{aligned} \quad (198)$$

$$= \frac{\alpha[I(\bar{V}; \bar{Y}) - I(\bar{V}; \bar{Z})]}{\alpha[I(\bar{V}; \bar{X}) - I(\bar{V}; \bar{Z})] + \alpha[D(Q_X||P_X) - D(Q_Y||P_Y)] + (1 - \alpha)[D(Q_{X|U=0}||P_X) - D(Q_{Y|U=0}||P_Y)]} \quad (199)$$

$$= \frac{I(\bar{V}; \bar{Y}) - I(\bar{V}; \bar{Z})}{I(\bar{V}; \bar{X}) - I(\bar{V}; \bar{Z}) + D(Q_X||P_X) - D(Q_Y||P_Y) + o(1)} \quad (200)$$

$$\frac{I(\bar{V}; \bar{Y}) - I(\bar{V}; \bar{Z})}{I(\bar{V}; \bar{X}) - I(\bar{V}; \bar{Z}) + D(Q_X||P_X) - D(Q_Y||P_Y)} \quad (203)$$

$$= \frac{\int [D(P_{\bar{Y}|\bar{V}=v}||P_Y) - D(P_{\bar{Z}|\bar{V}=v}||P_Z)] dP_{\bar{V}}(v) - D(P_{\bar{Y}}||P_Y) + D(P_{\bar{Z}}||P_Z)}{\int [D(P_{\bar{X}|\bar{V}=v}||P_X) - D(P_{\bar{Z}|\bar{V}=v}||P_Z)] dP_{\bar{V}}(v) - D(P_{\bar{Y}}||P_Y) + D(P_{\bar{Z}}||P_Z)} \quad (204)$$

$$\leq \frac{\int [D(P_{\bar{Y}|\bar{V}=v}||P_Y) - D(P_{\bar{Z}|\bar{V}=v}||P_Z)] dP_{\bar{V}}(v)}{\int [D(P_{\bar{X}|\bar{V}=v}||P_X) - D(P_{\bar{Z}|\bar{V}=v}||P_Z)] dP_{\bar{V}}(v)} \quad (205)$$

$$\leq \sup_{Q_X} \frac{D(Q_Y||P_Y) - D(Q_Z||P_Z)}{D(Q_X||P_X) - D(Q_Z||P_Z)}, \quad (206)$$

due to Leonard Gross [36], which illustrates the interesting connection between Gaussian and symmetric Bernoulli distributions.

APPENDIX E PROOF OF THEOREM 5

Recall the following facts from linear algebra (see for example [37]):

Fact 2. If \mathbf{A} and \mathbf{B} are matrices of the same dimension, then \mathbf{AB}^\top and $\mathbf{B}^\top\mathbf{A}$ have the same nonzero eigenvalues.

Fact 3. If \mathbf{A} is a square matrix, then

$$|\mathbf{I} + \epsilon\mathbf{A}| = \mathbf{I} + \epsilon \operatorname{tr}(\mathbf{A}) + O(\epsilon^2). \quad (231)$$

Now we are in the position of proving Theorem 5. Let $s := \lambda_{\max}((\mathbf{G} - \mathbf{H})(\mathbf{I} - \mathbf{H})^{-1})$. We first show that $s_{\mathbf{Z}}^*(\mathbf{X}; \mathbf{Y}) \geq s^+$. Since $s_{\mathbf{Z}}^*(\mathbf{X}; \mathbf{Y})$ is nonnegative we only need to focus on the case of $s \geq 0$. By restricting $Q_{V\mathbf{X}}$ in (43) to have the marginal distribution $P_{\mathbf{X}}$ on \mathcal{X} , we find

$$s_{\mathbf{Z}}^*(\mathbf{X}; \mathbf{Y}) \geq \sup_{P_{V|\mathbf{X}}} \frac{I(V; \mathbf{Y}) - I(V; \mathbf{Z})}{I(V; \mathbf{X}) - I(V; \mathbf{Z})}. \quad (232)$$

We remark that using Fact 1 one can actually show that (232) holds with equality, although we shall not use the “ \leq ” direction.

Let

$$(\mathbf{I} - \mathbf{H})^{-\frac{1}{2}}(\mathbf{G} - \mathbf{H})^{\frac{1}{2}}(\mathbf{I} - \mathbf{H})^{-\frac{1}{2}} = \mathbf{Q}\mathbf{\Lambda}\mathbf{Q}^\top \quad (233)$$

be the eigendecomposition of $(\mathbf{I} - \mathbf{H})^{-\frac{1}{2}}(\mathbf{G} - \mathbf{H})^{\frac{1}{2}}(\mathbf{I} - \mathbf{H})^{-\frac{1}{2}}$, where \mathbf{Q} is an orthogonal matrix and $\mathbf{\Lambda}$ is a diagonal matrix. Here we can take the square root of $\mathbf{I} - \mathbf{H}$ because it is a positive-semidefinite matrix according to Remark 5. By Fact 2, s is the largest eigenvalue of $(\mathbf{I} - \mathbf{H})^{-\frac{1}{2}}(\mathbf{G} - \mathbf{H})(\mathbf{I} - \mathbf{H})^{-\frac{1}{2}}$, hence we can assume without loss of generality that $\Lambda_{1,1} = s$. For each $\epsilon > 0$ define the $L \times L$ matrices

$$\mathbf{D}_\epsilon = \begin{pmatrix} \epsilon & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \quad (234)$$

and

$$\mathbf{\Delta}_\epsilon = (\mathbf{I} - \mathbf{H})^{-\frac{1}{2}}\mathbf{Q}\mathbf{D}_\epsilon\mathbf{Q}^\top(\mathbf{I} - \mathbf{H})^{-\frac{1}{2}}. \quad (235)$$

Choose \mathbf{V}_ϵ to be a random L -vector such that \mathbf{V}_ϵ and \mathbf{X} are jointly Gaussian, $\mathbf{V}_\epsilon - \mathbf{X} - (\mathbf{Y}, \mathbf{Z})$, and

$$\Sigma_{\mathbf{X}|\mathbf{V}_\epsilon} = \Sigma_{\mathbf{X}}^{\frac{1}{2}}(\mathbf{I} - \mathbf{\Delta}_\epsilon)\Sigma_{\mathbf{X}}^{\frac{1}{2}}. \quad (236)$$

This determines the joint distribution (up to a shift and a linear transform of \mathbf{V}_ϵ , which are irrelevant), since the unconditional covariance of \mathbf{X} is given in the problem statement. Then, observe that (see (237)-(240)): where the last step uses (236).

Hence,

$$\begin{aligned} I(\mathbf{V}_\epsilon; \mathbf{Y}) &= \frac{1}{2} \log \frac{|\Sigma_{\mathbf{Y}}|}{|\Sigma_{\mathbf{Y}|\mathbf{V}_\epsilon}|} \\ &= -\frac{1}{2} \log |\mathbf{I} - \Sigma_{\mathbf{Y}}^{-\frac{1}{2}}\Sigma_{\mathbf{YX}}\Sigma_{\mathbf{X}}^{-\frac{1}{2}}\mathbf{\Delta}_\epsilon\Sigma_{\mathbf{X}}^{-\frac{1}{2}}\Sigma_{\mathbf{XY}}\Sigma_{\mathbf{Y}}^{-\frac{1}{2}}| \end{aligned} \quad (241)$$

$$= -\frac{1}{2} \log |\mathbf{I} - \mathbf{G}\mathbf{\Delta}_\epsilon| \quad (242)$$

$$= -\frac{1}{2} \log |\mathbf{I} - \mathbf{G}\mathbf{\Delta}_\epsilon| \quad (243)$$

$$= \frac{\log e}{2} \operatorname{tr}(\mathbf{G}\mathbf{\Delta}_\epsilon) + O(\epsilon^2) \quad (244)$$

where (243) uses Fact 2 (or the Sylvester determinant identity) and (244) uses Fact 3. By the same token, we have shown

$$I(\mathbf{V}_\epsilon; \mathbf{X}) = \frac{\log e}{2} \operatorname{tr}(\mathbf{\Delta}_\epsilon) + O(\epsilon^2) \quad (245)$$

and

$$I(\mathbf{V}_\epsilon; \mathbf{Z}) = \frac{\log e}{2} \operatorname{tr}(\mathbf{H}\mathbf{\Delta}_\epsilon) + O(\epsilon^2). \quad (246)$$

Therefore,

$$\begin{aligned} \lim_{\epsilon \downarrow 0} \frac{I(\mathbf{V}_\epsilon; \mathbf{Y}) - I(\mathbf{V}_\epsilon; \mathbf{Z})}{I(\mathbf{V}_\epsilon; \mathbf{X}) - I(\mathbf{V}_\epsilon; \mathbf{Z})} &= \lim_{\epsilon \downarrow 0} \frac{\operatorname{tr}((\mathbf{G} - \mathbf{H})\mathbf{\Delta}_\epsilon)}{\operatorname{tr}((\mathbf{I} - \mathbf{H})\mathbf{\Delta}_\epsilon)} \end{aligned} \quad (247)$$

$$= \lim_{\epsilon \downarrow 0} \frac{\operatorname{tr}\left((\mathbf{G} - \mathbf{H})(\mathbf{I} - \mathbf{H})^{-\frac{1}{2}}\mathbf{Q}\mathbf{D}_\epsilon\mathbf{Q}^\top(\mathbf{I} - \mathbf{H})^{-\frac{1}{2}}\right)}{\operatorname{tr}(\mathbf{D}_\epsilon)} \quad (248)$$

$$= \lim_{\epsilon \downarrow 0} \frac{\operatorname{tr}(\mathbf{\Lambda}\mathbf{D}_\epsilon)}{\operatorname{tr}(\mathbf{D}_\epsilon)} \quad (249)$$

$$= \Lambda_{1,1} \quad (250)$$

$$= s, \quad (251)$$

Hence by (232) we have shown that $s_{\mathbf{Z}}^*(\mathbf{X}; \mathbf{Y}) \geq s = s^+$.

Conversely, to show $s_{\mathbf{Z}}^*(\mathbf{X}; \mathbf{Y}) \leq s^+$, we may assume without loss of generality that $s < 1$ since Remark 5 implies that $s \leq 1$ and when $s = 1$ the claim is trivially true. We have remarked that s is the largest eigenvalue of $(\mathbf{I} - \mathbf{H})^{-\frac{1}{2}}(\mathbf{G} - \mathbf{H})(\mathbf{I} - \mathbf{H})^{-\frac{1}{2}}$, hence

$$(\mathbf{I} - \mathbf{H})^{-\frac{1}{2}}(\mathbf{G} - \mathbf{H})(\mathbf{I} - \mathbf{H})^{-\frac{1}{2}} \preceq s\mathbf{I}, \quad (252)$$

which implies

$$\mathbf{I} - \mathbf{G} \succeq (1 - s)(\mathbf{I} - \mathbf{H}). \quad (253)$$

Now define $\hat{\mathbf{H}} := \mathbf{I} - \frac{1}{1-s}(\mathbf{I} - \mathbf{G})$, then

$$\mathbf{I} - \mathbf{G} = (1 - s)(\mathbf{I} - \hat{\mathbf{H}}). \quad (254)$$

From (253) and (254) it is clear that

$$\hat{\mathbf{H}} \preceq \mathbf{H}. \quad (255)$$

By (255), we can find a Gaussian L -vector \mathbf{W} independent of $(\mathbf{X}, \mathbf{Y}, \mathbf{Z})$ and define

$$\hat{\mathbf{Z}} = \mathbf{Z} + \mathbf{W} \quad (256)$$

such that

$$\hat{\mathbf{H}} = \Sigma_{\mathbf{X}}^{-1/2}\Sigma_{\mathbf{XZ}}\Sigma_{\hat{\mathbf{Z}}}^{-1}\Sigma_{\mathbf{ZX}}\Sigma_{\mathbf{X}}^{-1/2}. \quad (257)$$

Since $\mathbf{X} \perp \mathbf{W}$, we see that

$$\hat{\mathbf{H}} = \Sigma_{\mathbf{X}}^{-1/2} \Sigma_{\mathbf{X}\hat{\mathbf{Z}}} \Sigma_{\hat{\mathbf{Z}}}^{-1} \Sigma_{\hat{\mathbf{Z}}\mathbf{X}} \Sigma_{\mathbf{X}}^{-1/2}, \quad (258)$$

which agrees with the definition (34), i.e. $\hat{\mathbf{H}}$ is the corresponding matrix for the source $(\mathbf{X}, \mathbf{Y}, \hat{\mathbf{Z}})$. A noisier observation for the eavesdropper is advantageous for key generation, hence $\eta_{\hat{\mathbf{Z}}}(\mathbf{X}; \mathbf{Y}) \geq \eta_{\mathbf{Z}}(\mathbf{X}; \mathbf{Y})$, and so $s_{\hat{\mathbf{Z}}}^*(\mathbf{X}; \mathbf{Y}) \geq s_{\mathbf{Z}}^*(\mathbf{X}; \mathbf{Y})$. Moreover from (254) we see that $\hat{\mathbf{H}}$ commutes with \mathbf{G} , so that we can apply Lemma 1 to find invertible linear transforms $\mathbf{X} \mapsto \bar{\mathbf{X}}, \mathbf{Y} \mapsto \bar{\mathbf{Y}}, \hat{\mathbf{Z}} \mapsto \bar{\mathbf{Z}}$ such that $(\bar{\mathbf{X}}, \bar{\mathbf{Y}}, \bar{\mathbf{Z}})$ is a product source in the sense of (1) and (2). Furthermore, from the proof of Lemma 1 one sees that

$$1 - \rho_{\bar{\mathbf{X}}_i \bar{\mathbf{Y}}_i} = (1 - s)(1 - \rho_{\bar{\mathbf{X}}_i \bar{\mathbf{Z}}_i}) \quad (259)$$

for $i = 1, \dots, L$. Hence by (42),

$$s_{\hat{\mathbf{Z}}}^*(\mathbf{X}; \mathbf{Y}) = s_{\bar{\mathbf{Z}}}^*(\bar{\mathbf{X}}; \bar{\mathbf{Y}}) \quad (260)$$

$$= s_{\bar{\mathbf{Z}}_i}^*(\bar{\mathbf{X}}_i; \bar{\mathbf{Y}}_i) \quad (261)$$

$$= \left(\frac{\rho_{\bar{\mathbf{X}}_i \bar{\mathbf{Y}}_i} - \rho_{\bar{\mathbf{X}}_i \bar{\mathbf{Z}}_i}}{1 - \rho_{\bar{\mathbf{X}}_i \bar{\mathbf{Z}}_i}} \right)^+ \quad (262)$$

$$= s^+, \quad (263)$$

and we can conclude that

$$s_{\mathbf{Z}}^*(\mathbf{X}; \mathbf{Y}) \leq s_{\hat{\mathbf{Z}}}^*(\mathbf{X}; \mathbf{Y}) \leq s^+. \quad (264)$$

In summary we have shown that $s_{\mathbf{Z}}^*(\mathbf{X}; \mathbf{Y}) = s^+$, or equivalently

$$\eta_{\mathbf{Z}}(\mathbf{X}; \mathbf{Y}) = \frac{s^+}{1 - s^+} = \left(\frac{s}{1 - s} \right)^+ = \lambda_{\max}^+((\mathbf{G} - \mathbf{H})(\mathbf{I} - \mathbf{G})^{-1}), \quad (265)$$

as desired.

APPENDIX F PROOF OF LEMMA 3

From Jensen's inequality we have

$$\ln \mathbb{E} e^{t\eta} \geq \mathbb{E} \ln e^{t\eta} = t\mathbb{E}\eta. \quad (266)$$

The proof of the other part of the bound in (132) is essentially based on uniform integrability of $\{e^{t\eta}\}_{\rho \in [0, 1-\delta]}$. Without loss of generality we can assume that U, X are zero mean with unit variance. Also it suffices to consider only the case of $\rho \geq 0$ since otherwise the correlation coefficient between $-U$ and X is $-\rho > 0$ but the distribution of $\iota_{-U; X}(-U; X)$ is the

same as that of η . Now $N := \frac{X - \rho U}{\sqrt{1 - \rho^2}}$ is zero mean, with unit variance, and independent of U . Note that

$$|\eta| = \left| \frac{1}{2} \log \frac{1}{1 - \rho^2} - \frac{1}{2} \log e \left(\frac{\rho^2 U^2 + \rho^2 X^2}{1 - \rho^2} - \frac{2\rho U X}{1 - \rho^2} \right) \right| \quad (267)$$

$$\leq \frac{1}{2} \log \frac{1}{1 - \rho^2} + \frac{1}{2} \log e \cdot \frac{\rho^2 U^2 + \rho^2 X^2 + \rho(U^2 + X^2)}{1 - \rho^2} \quad (268)$$

$$\leq \frac{1}{2} \log \frac{1}{1 - \rho^2} + \frac{1}{2} \log e \cdot \frac{\rho(U^2 + X^2)}{1 - \rho} \quad (269)$$

$$\leq \frac{1}{2} \log \frac{1}{1 - \rho^2} + \frac{\rho \log e}{2\delta} (U^2 + X^2) \quad (270)$$

$$= \frac{1}{2} \log \frac{1}{1 - \rho^2} + \frac{\rho \log e}{2\delta} [U^2 + (\sqrt{1 - \rho^2} N + \rho U)^2] \quad (271)$$

$$\leq \frac{1}{2} \log \frac{1}{1 - \rho^2} + \frac{3\rho \log e}{2\delta} (U^2 + N^2) \quad (272)$$

$$\leq \frac{1}{2} \log \frac{1}{1 - (1 - \delta)^2} + \frac{3 \log e}{2\delta} (U^2 + N^2). \quad (273)$$

It is easy to show that for any $\lambda < \frac{1}{4}$, $\mathbb{E} e^{2\lambda U^2} = \mathbb{E} e^{2\lambda N^2}$ is finite, and hence

$$\mathbb{E}[e^{\lambda U^2} e^{\lambda N^2}] \leq \sqrt{\mathbb{E} e^{2\lambda U^2} \mathbb{E} e^{2\lambda N^2}} \quad (274)$$

$$< \infty. \quad (275)$$

Let ξ be the random variable in (273), whose distribution does not depend on ρ . By (275), $\mathbb{E} e^{t\xi} < \infty$ for all $0 < t < \frac{\delta}{6 \log e}$. Now for each $\delta > 0$,

$$\lim_{\Delta \rightarrow \infty} \sup_{\rho \in [0, 1-\delta], t \in (0, \frac{\delta}{7 \log e}]} \mathbb{E} 1_{|\eta| \geq \Delta} e^{t\eta} \leq \lim_{\Delta \rightarrow \infty} \sup_{\rho \in [0, 1-\delta], t \in (0, \frac{\delta}{7 \log e}]} \mathbb{E} 1_{|\eta| \geq \Delta} e^{t|\eta|} \quad (276)$$

$$\leq \lim_{\Delta \rightarrow \infty} \sup_{t \in (0, \frac{\delta}{7 \log e}]} \mathbb{E} 1_{\xi \geq \Delta} e^{t\xi} \quad (277)$$

$$\leq \lim_{\Delta \rightarrow \infty} \mathbb{E} 1_{\xi \geq \Delta} \exp \left(\frac{\delta \xi}{7 \log e} \right) \quad (278)$$

$$= 0 \quad (279)$$

where the last step follows from bounded convergence theorem (or dominated convergence theorem). Then there exists $\Delta_0 > 0$ large enough such that

$$\sup_{\rho \in [0, 1-\delta], t \in (0, \frac{\delta}{7 \log e}]} \mathbb{E} 1_{|\eta| \geq \Delta} e^{t\eta} < \frac{\epsilon}{4}, \quad (280)$$

$$\mathbb{P}[\xi < \Delta_0] > \frac{1}{2}. \quad (281)$$

$$\Sigma_{\mathbf{Y}|\mathbf{V}_\epsilon} = \Sigma_{\mathbf{Y}|\mathbf{X}} + \mathbb{E}[(\mathbb{E}[\mathbf{Y}|\mathbf{X}] - \mathbb{E}[\mathbf{Y}|\mathbf{V}_\epsilon])(\mathbb{E}[\mathbf{Y}|\mathbf{X}] - \mathbb{E}[\mathbf{Y}|\mathbf{V}_\epsilon])^\top | \mathbf{V}_\epsilon] \quad (287)$$

$$= \Sigma_{\mathbf{Y}|\mathbf{X}} + \mathbb{E}[\Sigma_{\mathbf{YX}} \Sigma_{\mathbf{X}}^{-1} (\mathbf{X} - \mathbb{E}[\mathbf{X}|\mathbf{V}_\epsilon])(\mathbf{X} - \mathbb{E}[\mathbf{X}|\mathbf{V}_\epsilon])^\top \Sigma_{\mathbf{X}}^{-1} \Sigma_{\mathbf{XY}} | \mathbf{V}_\epsilon] \quad (288)$$

$$= \Sigma_{\mathbf{Y}|\mathbf{X}} + \Sigma_{\mathbf{YX}} \Sigma_{\mathbf{X}}^{-1} \Sigma_{\mathbf{X}|\mathbf{V}_\epsilon} \Sigma_{\mathbf{X}}^{-1} \Sigma_{\mathbf{XY}} \quad (289)$$

$$= \Sigma_{\mathbf{Y}} - \Sigma_{\mathbf{YX}} \Sigma_{\mathbf{X}}^{-\frac{1}{2}} \Delta_\epsilon \Sigma_{\mathbf{X}}^{-\frac{1}{2}} \Sigma_{\mathbf{XY}} \quad (290)$$

for $\Delta \geq \Delta_0$. Now observe that from (272), there exists a r.v. $\zeta = C_1(U^2 + N^2) + C_2$ such that $|\eta| < \rho\zeta$ whenever $\rho < \frac{1}{2}$, where C_1, C_2 are constants depending only on δ . Then,

$$\sup_{t < \frac{1}{2}} \sup_{\rho < \delta_0} \frac{\ln \mathbb{E} e^{t\eta}}{t} \leq \sup_{t < \frac{1}{2}} \sup_{\rho < \delta_0} \frac{\ln \mathbb{E} e^{\rho t \zeta}}{t} \quad (282)$$

$$= \sup_{t < \frac{1}{2}} \frac{\ln \mathbb{E} e^{\delta_0 t \zeta}}{t} \quad (283)$$

$$= 2 \ln \mathbb{E} e^{\frac{\delta_0 \zeta}{2}} \quad (284)$$

$$\rightarrow 0, \quad \delta_0 \rightarrow 0, \quad (285)$$

where (284) follows from convexity of the cumulant generating function. Thus, we can pick δ_0 small enough such that

$$\sup_{t < \frac{1}{2}} \sup_{\rho < \delta_0} \frac{\ln \mathbb{E} e^{t\eta}}{t} \leq \epsilon. \quad (286)$$

On the other hand, for $\rho \geq \delta_0$ we have

$$\begin{aligned} & \sup_{\delta_0 \leq \rho < 1-\delta} \frac{\ln \mathbb{E} e^{t\eta}}{t \mathbb{E} \eta} \\ &= \sup_{\delta_0 \leq \rho < 1-\delta} \frac{\ln(\mathbb{E} 1_{|\eta| \geq \Delta_0} e^{t\eta} + \mathbb{E} 1_{|\eta| < \Delta_0} e^{t\eta})}{t \mathbb{E} \eta} \end{aligned} \quad (287)$$

$$\leq \sup_{\delta_0 \leq \rho < 1-\delta} \frac{\ln \mathbb{E} 1_{|\eta| < \Delta_0} e^{t\eta}}{t \mathbb{E} \eta} \left(1 + \frac{\mathbb{E} 1_{|\eta| \geq \Delta_0} e^{t\eta}}{\mathbb{E} 1_{|\eta| < \Delta_0} e^{t\eta}} \right) \quad (288)$$

$$\leq \sup_{\delta_0 \leq \rho < 1-\delta} \left\{ \frac{\ln[(\mathbb{E} t\eta + 1) \cdot \beta_t]}{t \mathbb{E} \eta} \left(1 + \frac{\epsilon/4}{e^{-t\Delta_0} \mathbb{P}[|\eta| < \Delta_0]} \right) \right\} \quad (289)$$

$$\leq \sup_{\delta_0 \leq \rho < 1-\delta} \left\{ \frac{\mathbb{E} t\eta + \ln \beta_t}{t \mathbb{E} \eta} \left(1 + \frac{\epsilon}{2} e^{t\Delta_0} \right) \right\} \quad (290)$$

$$\leq \sup_{\delta_0 \leq \rho < 1-\delta} \left\{ \left(1 + \frac{\ln \beta_t}{t \cdot \frac{1}{2} \log \frac{1}{1-\delta_0^2}} \left(1 + \frac{\epsilon}{2} e^{t\Delta_0} \right) \right) \right\} \quad (291)$$

$$\rightarrow 1 + \epsilon/2, \quad t \rightarrow 0. \quad (292)$$

where we have defined $\beta_t := \max\{\frac{e^{t\Delta_0}}{1+t\Delta_0}, \frac{e^{-t\Delta_0}}{1-t\Delta_0}\}$, and used the fact that $\beta_t = 1 + O(t^2)$ when $t \rightarrow 0$. Finally, in view of (286) and (292), there exist $t < \frac{1}{2}$ small enough such that for each $\rho \in [0, 1-\delta]$, either $\ln \mathbb{E} e^{t\eta} < t\epsilon$ or $\ln \mathbb{E} e^{t\eta} < (1+\epsilon)\mathbb{E} t\eta$ hold.

APPENDIX G PROOF OF LEMMA 5

- (a) The asymptotic equivalences have been remarked earlier in (121), so we only have to bound the eigenvalues. From [23, Lemma 4.1] we have

$$\begin{aligned} 0 &< \min_{\omega \in [0, 2\pi)} S_X(\omega) \\ &\leq \lambda_{\min}(\Sigma_X) \\ &\leq \lambda_{\max}(\Sigma_X) \\ &\leq \max_{\omega \in [0, 2\pi)} S_X(\omega); \end{aligned} \quad (293)$$

from (115) the eigenvalues of $\Sigma_{\tilde{X}}$ are $\{S_X(\frac{2\pi k}{n})\}_{k=1}^n$, which are also bounded between $\min_{\omega \in [0, 2\pi)} S_X(\omega)$ and $\max_{\omega \in [0, 2\pi)} S_X(\omega)$. Similarly, the eigenvalues of $\Sigma_{\tilde{Y}}$ and Σ_Y

are bounded between $\min_{\omega \in [0, 2\pi)} S_Y(\omega)$ and $\max_{\omega \in [0, 2\pi)} S_Y(\omega)$; and the eigenvalues of $\Sigma_{\tilde{Z}}$ and Σ_Z are bounded between $\min_{\omega \in [0, 2\pi)} S_Z(\omega)$ and $\max_{\omega \in [0, 2\pi)} S_Z(\omega)$.

We first show that $\Sigma_{X|U} \sim \Sigma_{\tilde{X}|\hat{U}}$. Let \mathbf{R} be the diagonal matrix whose (i, i) entry is $\rho_i^{(n)}$. Clearly both $\Sigma_{X|U}$ and $\Sigma_{\tilde{X}|\hat{U}}$ depend only on \mathbf{R} and $\Sigma_{\tilde{X}}$, and do not depend on the scaling of \hat{U} . However, to compute $\Sigma_{\tilde{X}|\hat{U}}$, it is convenient to specify $P_{\hat{U}|\tilde{X}}$ via the following random transformation:

$$\hat{U} = (\mathbf{I} - \mathbf{R}^2)^{\frac{1}{2}} \mathbf{W} + \mathbf{R} \hat{\mathbf{X}}, \quad (294)$$

where \mathbf{W} is a zero mean Gaussian vector with covariance matrix $\Sigma_{\tilde{X}}$ and independent of $\hat{\mathbf{X}}$. Then the conditional covariance matrices can be expressed as

$$\Sigma_{\tilde{X}|\hat{U}} = \Sigma_{\tilde{X}} - \Sigma_{\tilde{X}\hat{U}} \Sigma_{\hat{U}}^{-1} \Sigma_{\hat{U}\tilde{X}} \quad (295)$$

$$\begin{aligned} &= \Sigma_{\tilde{X}} - \Sigma_{\tilde{X}} \mathbf{Q} \mathbf{R} [(\mathbf{I} - \mathbf{R}^2)^{\frac{1}{2}} \Sigma_{\tilde{X}} (\mathbf{I} - \mathbf{R}^2)^{\frac{1}{2}} \\ &\quad + \mathbf{R} \mathbf{Q}^\top \Sigma_{\tilde{X}} \mathbf{Q} \mathbf{R}]^{-1} \mathbf{R} \mathbf{Q}^\top \Sigma_{\tilde{X}}. \end{aligned} \quad (296)$$

and

$$\Sigma_{X|U} = \Sigma_X - \Sigma_{XU} \Sigma_U^{-1} \Sigma_{UX} \quad (297)$$

$$\begin{aligned} &= \Sigma_X - \Sigma_X \mathbf{Q} \mathbf{R} [(\mathbf{I} - \mathbf{R}^2)^{\frac{1}{2}} \Sigma_{\tilde{X}} (\mathbf{I} - \mathbf{R}^2)^{\frac{1}{2}} \\ &\quad + \mathbf{R} \mathbf{Q}^\top \Sigma_X \mathbf{Q} \mathbf{R}]^{-1} \mathbf{R} \mathbf{Q}^\top \Sigma_X. \end{aligned} \quad (298)$$

It is easy to see that the smallest eigenvalue of $(\mathbf{I} - \mathbf{R}^2)^{\frac{1}{2}} \Sigma_{\tilde{X}} (\mathbf{I} - \mathbf{R}^2)^{\frac{1}{2}}$ is lower bounded by $\min_{\omega \in [0, 2\pi)} S_X(\omega) (1 - \max_{\omega \in [0, 2\pi)} \rho_{UX}^2(\omega))$ which is positive due to (140). Therefore, Fact 5 and Part (a) imply the asymptotic equivalence $\Sigma_{X|U} \sim \Sigma_{\tilde{X}|\hat{U}}$.

Next, from the Markov chains $U - X - Y$ and $\hat{U} - \tilde{X} - \tilde{Y}$, we can show that (similar to the derivations in (240))

$$\begin{aligned} \Sigma_{Y|U} &= \Sigma_{Y|X} + \Sigma_{YX} \Sigma_X^{-1} \Sigma_{X|U} \Sigma_X^{-1} \Sigma_{XY} \\ &= \Sigma_Y - \Sigma_{YX} \Sigma_X^{-1} \Sigma_{XY} \\ &\quad + \Sigma_{YX} \Sigma_X^{-1} \Sigma_{X|U} \Sigma_X^{-1} \Sigma_{XY} \end{aligned} \quad (299)$$

and

$$\begin{aligned} \Sigma_{\tilde{Y}|\hat{U}} &= \Sigma_{\tilde{Y}} - \Sigma_{\tilde{Y}\tilde{X}} \Sigma_{\tilde{X}}^{-1} \Sigma_{\tilde{X}\tilde{Y}} \\ &\quad + \Sigma_{\tilde{Y}\tilde{X}} \Sigma_{\tilde{X}}^{-1} \Sigma_{\tilde{X}|\hat{U}} \Sigma_{\tilde{X}}^{-1} \Sigma_{\tilde{X}\tilde{Y}}. \end{aligned} \quad (300)$$

Therefore (121), $\Sigma_{X|U} \sim \Sigma_{\tilde{X}|\hat{U}}$, and Part (a) immediately establish the relation $\Sigma_{Y|U} \sim \Sigma_{\tilde{Y}|\hat{U}}$.

Note that (299) can be written as

$$\Sigma_{Y|U} = \Sigma_Y^{\frac{1}{2}} [\mathbf{I} - \mathbf{A} (\mathbf{I} - \Sigma_X^{-\frac{1}{2}} \Sigma_{X|U} \Sigma_X^{-\frac{1}{2}}) \mathbf{A}^\top] \Sigma_Y^{\frac{1}{2}}, \quad (301)$$

where we have defined $\mathbf{A} = \Sigma_Y^{-\frac{1}{2}} \Sigma_{YX} \Sigma_X^{-\frac{1}{2}}$. From the result of Part (a) we see that

$$\lambda_{\max}(\mathbf{I} - \Sigma_X^{-\frac{1}{2}} \Sigma_{X|U} \Sigma_X^{-\frac{1}{2}}) < 1 - \delta \quad (302)$$

for some $\delta > 0$ which is independent of n . However the positive-semidefiniteness of the covariance

matrix of $(\mathbf{X}^\top, \mathbf{Y}^\top)$ implies that the largest singular value $\sigma_{\max}(\mathbf{A}) \leq 1$, which in turn gives

$$\lambda_{\max}(\mathbf{A}(\mathbf{I} - \Sigma_{\mathbf{X}}^{-\frac{1}{2}}\Sigma_{\mathbf{X}|\mathbf{U}}\Sigma_{\mathbf{X}}^{-\frac{1}{2}})\mathbf{A}^\top) < 1 - \delta. \quad (303)$$

Therefore we have the uniform lower bound

$$\lambda_{\min}(\Sigma_{\mathbf{Y}|\mathbf{U}}) \geq \min_{\omega \in [0, 2\pi)} S_Y(\omega) \quad (304)$$

$$(1 - \lambda_{\max}(\mathbf{A}(\mathbf{I} - \Sigma_{\mathbf{X}}^{-\frac{1}{2}}\Sigma_{\mathbf{X}|\mathbf{U}}\Sigma_{\mathbf{X}}^{-\frac{1}{2}})\mathbf{A}^\top)) \quad (305)$$

$$> \delta \min_{\omega \in [0, 2\pi)} S_Y(\omega), \quad \forall n > 0. \quad (306)$$

A similar uniform lower bound can be obtained for $\Sigma_{\hat{\mathbf{Y}}|\hat{\mathbf{U}}}$. The relation $\Sigma_{\mathbf{Z}|\mathbf{U}} \sim \Sigma_{\hat{\mathbf{Z}}|\hat{\mathbf{U}}}$ and the uniform lower boundedness of their eigenvalues can be shown in the exactly same way since the roles of \mathbb{Y} and \mathbb{Z} are equal for this problem.

APPENDIX H CONVERSE OF THEOREM 6

The first step towards the converse proof is to bound the key rate and the transmission rate with multi-letter expressions. This part is similar to the initial steps in the converse proof of key capacity of memoryless sources, c.f. [1].

Consider

$$\log |\mathcal{K}| = H(K|W, Z^n) + \nu_n \quad (307)$$

$$\leq H(K) + \nu_n \quad (308)$$

$$\leq H(K) - H(K|Y^n, W) + n\gamma_n + \nu_n \quad (309)$$

$$= I(K; Y^n, W) + n\gamma_n + \nu_n \quad (310)$$

$$\leq I(K; Y^n, W) - I(K; Z^n, W) + n\gamma_n + 2\nu_n \quad (311)$$

$$= I(K; Y^n|W) - I(K; Z^n|W) + n\gamma_n + 2\nu_n, \quad (312)$$

where (308) and (311) are from the definition of ν_n and (309) is from Fano's inequality, with $\gamma_n := \frac{1}{n}[\epsilon_n \log |\mathcal{K}_1| + h(\epsilon_n)]$.

As for the transmission rate, note that

$$\log |\mathcal{W}| \geq H(W) \quad (313)$$

$$\geq H(W|Y^n) - H(W, K|X^n) \quad (314)$$

$$\geq H(W|Y^n) + H(K|W, Y^n) - n\gamma_n - H(W, K|X^n) \quad (315)$$

$$= H(K, W|Y^n) - n\gamma_n - H(W, K|X^n) \quad (316)$$

$$= I(K, W; X^n) - I(K, W; Y^n) - n\gamma_n, \quad (317)$$

where (315) used Fano's inequality.

Now suppose (R, r) is achievable, where $r > 0, R > 0$. We identify K and W in (312), (317) with V, U respectively, and then apply Fact 1. Also notice that $\lim_{n \rightarrow 0} \gamma_n = \lim_{n \rightarrow \infty} \nu_n = 0$. These imply the existence of a sequence of conditional Gaussian distributions $P_{U^n|X^n}$ such that

$$r \geq \lim_{n \rightarrow \infty} \frac{1}{n} [I(X^n; U^n) - I(Y^n; U^n)]; \quad (318)$$

$$R \leq \lim_{n \rightarrow \infty} \frac{1}{n} [I(Y^n; U^n) - I(Z^n; U^n)]. \quad (319)$$

As in Section V, let $\tilde{\mathbf{X}}, \tilde{\mathbf{Y}}$ and $\tilde{\mathbf{Z}}$ be jointly Gaussian vectors with circulant covariance matrices defined in (120); and $\hat{\mathbf{X}}, \hat{\mathbf{Y}}, \hat{\mathbf{Z}}$ be the result of applying the linear transforms in (122)-(124). Then

$$r \geq \lim_{n \rightarrow \infty} \frac{1}{n} [I(\hat{\mathbf{X}}; \hat{\mathbf{U}}) - I(\hat{\mathbf{Y}}; \hat{\mathbf{U}})]; \quad (320)$$

$$R \leq \lim_{n \rightarrow \infty} \frac{1}{n} [I(\hat{\mathbf{Y}}; \hat{\mathbf{U}}) - I(\hat{\mathbf{Z}}; \hat{\mathbf{U}})]. \quad (321)$$

For $x > 0$ define the decreasing functions:

$$f(x) = \frac{1}{4\pi} \int_{\beta(\omega) > x} \log \frac{\beta(\omega)(x+1)}{(\beta(\omega)+1)x} d\omega, \quad (322)$$

$$g(x) = \frac{1}{4\pi} \int_{\beta(\omega) > x} \log \frac{\beta(\omega)+1}{x+1} d\omega, \quad (323)$$

$$f_n(x) := \frac{1}{2n} \sum_{i: \beta_i^{(n)} > x} \log \frac{\beta_i^{(n)}(x+1)}{(\beta_i^{(n)}+1)x}, \quad (324)$$

$$g_n(x) := \frac{1}{2n} \sum_{i: \beta_i^{(n)} > x} \log \frac{\beta_i^{(n)}+1}{x+1}, \quad (325)$$

where

$$\beta_i^{(n)} := \frac{\rho_{\hat{\mathbf{X}}_i^{(n)} \hat{\mathbf{Y}}_i^{(n)}}^2 - \rho_{\hat{\mathbf{X}}_i^{(n)} \hat{\mathbf{Z}}_i^{(n)}}^2}{1 - \rho_{\hat{\mathbf{X}}_i^{(n)} \hat{\mathbf{Y}}_i^{(n)}}^2}. \quad (326)$$

The empirical distribution of $\{\beta_i^{(n)}\}_{i=1}^n$ converges weakly to the distribution of $\beta(W)$ when W is uniformly distributed on $[0, 2\pi)$, which means that for any $x > 0$ it holds that

$$\lim_{n \rightarrow \infty} f_n(x) = f(x), \quad (327)$$

$$\lim_{n \rightarrow \infty} g_n(x) = g(x). \quad (328)$$

By Theorem 2, there is a sequence $\{\mu_n\}$ such that $I(\hat{\mathbf{X}}; \hat{\mathbf{U}}) - I(\hat{\mathbf{Y}}; \hat{\mathbf{U}}) \geq f_n(\mu_n)$ and $I(\hat{\mathbf{Y}}; \hat{\mathbf{U}}) - I(\hat{\mathbf{Z}}; \hat{\mathbf{U}}) \leq g_n(\mu_n)$, and so

$$r \geq \limsup_{n \rightarrow \infty} f_n(\mu_n), \quad (329)$$

$$R \leq \liminf_{n \rightarrow \infty} g_n(\mu_n), \quad (330)$$

Define $\mu := \limsup_{n \rightarrow \infty} \mu_n$. We observe that μ_n is bounded away from 0 and $+\infty$: suppose on the contrary that it is not bounded away from 0. Choose $\epsilon > 0$ small enough such that $f(\epsilon) - \epsilon > r$ (which is possible since $\lim_{\epsilon \downarrow 0} f(\epsilon) = +\infty$ by monotone convergence theorem), and there is a subsequence $\{\mu_{n_k}\}_{k=1}^\infty$ such that $\mu_{n_k} < \epsilon$ for all k . From monotonicity of f_n we see that

$$f_{n_k}(\mu_{n_k}) \geq f_{n_k}(\epsilon) \rightarrow f(\epsilon), \quad k \rightarrow \infty. \quad (331)$$

This implies that $f_{n_k}(\mu_{n_k}) > f(\epsilon) - \epsilon > r$ when k is sufficiently large, which contradicts (329). Similarly we can also show that μ_n is upper bounded: if otherwise, we pick $M > 0$ such that $g(M) < \frac{R}{2}$ (which is possible since $\lim_{x \rightarrow +\infty} g(x) = 0$ by monotone convergence theorem), and choose a subsequence $\{\mu_{n_k}\}_{k=1}^\infty$ such that $\mu_{n_k} > M$ for all k . Then from monotonicity of g_n we see that

$$g_{n_k}(\mu_{n_k}) \leq g_{n_k}(M) \rightarrow g(M) < \frac{R}{2}, \quad k \rightarrow \infty. \quad (332)$$

This implies that $g_{n_k}(\mu_{n_k}) \leq \frac{3}{4}R$ for k large enough, which contradicts (330). Thus, we may assume that $c < \mu_n < d$, for some $0 < c < d$.

By differentiation it's easy to see that f_n is $\frac{\log e}{2c(1+c)}$ -Lipschitz on $[c, d]$. Now choose a new subsequence $\{\mu_{i_k}\}_{k=1}^\infty$ which converges to μ . We have

$$|f_{i_k}(\mu_{i_k}) - f(\mu)| \leq |f_{i_k}(\mu_{i_k}) - f_{i_k}(\mu)| + |f_{i_k}(\mu) - f(\mu)| \quad (333)$$

$$\leq \frac{\log e}{2c(1+c)}|\mu_{i_k} - \mu| + |f_{i_k}(\mu) - f(\mu)| \quad (334)$$

$$\rightarrow 0, \quad k \rightarrow \infty. \quad (335)$$

where (335) used (327). Hence

$$\liminf_{n \rightarrow \infty} f_n(\mu_n) \leq \lim_{k \rightarrow \infty} f_{i_k}(\mu_{i_k}) = f(\mu). \quad (336)$$

Similarly to (333)-(336), we can also show that

$$\limsup_{n \rightarrow \infty} g_n(\mu_n) \leq \lim_{k \rightarrow \infty} g_{i_k}(\mu_{i_k}) = g(\mu). \quad (337)$$

The proof is accomplished by combining (329), (330), (336) and (337).

APPENDIX I

REVIEW OF RESULTS ON TOEPLITZ APPROXIMATION

The asymptotic distribution of the eigenvalues of Toeplitz matrices can be described in terms of the “equal distribution” introduced by H. Weyl [38].

Definition 1. [39] For each n consider two sets of n real numbers $\{a_i^{(n)}\}_{i=1}^n$ and $\{b_i^{(n)}\}_{i=1}^n$ satisfying

$$A < a_i^{(n)} < B, \quad A < b_i^{(n)} < B, \quad \forall 1 \leq i \leq n, \quad n \geq 1. \quad (338)$$

for some $A, B > 0$. The sequences $\{a_i^{(n)}\}_{i=1}^n$ and $\{b_i^{(n)}\}_{i=1}^n$ are said to be *asymptotically equally distributed* in $[A, B]$ if for any continuous function $F: [A, B] \rightarrow \mathbb{R}$, it holds that

$$\lim_{n \rightarrow \infty} \frac{\sum_{i=1}^n [F(a_i^{(n)}) - F(b_i^{(n)})]}{n} = 0. \quad (339)$$

Denote by $\mathbb{P}_{a^{(n)}}$ the empirical distribution of $\{a^{(n)}\}$. Then (339) can be expressed as

$$\lim_{n \rightarrow \infty} [\mathbb{E}F(X_a) - \mathbb{E}F(X_b)] = 0, \quad (340)$$

where the random variables X_a and X_b are distributed according to $\mathbb{P}_{a^{(n)}}$ and $\mathbb{P}_{b^{(n)}}$, respectively.

Definition 2. Consider the sets $\{a_i^{(n)}\}_{i=1}^n$ of real numbers from $[A, B]$. The empirical distribution $\mathbb{P}_{a^{(n)}}$ is said to *converge weakly* to a measure μ on $[A, B]$ if for any continuous function $F: [A, B] \rightarrow \mathbb{R}$,

$$\lim_{n \rightarrow \infty} \mathbb{E}F(X_a) = \mathbb{E}F(X_\mu), \quad (341)$$

where the random variables X_a and X_μ are distributed according to $\mathbb{P}_{a^{(n)}}$ and μ , respectively.

Definition 3. [23] We say \mathbf{A}_n and \mathbf{B}_n are *asymptotically equivalent* (denoted as $\mathbf{A}_n \sim \mathbf{B}_n$) for two sequences of matrices $\{\mathbf{A}_n\}$ and $\{\mathbf{B}_n\}$ if

- 1) \mathbf{A}_n and \mathbf{B}_n are uniformly bounded in ℓ_2 operator norm, i.e. for some $M > 0$,

$$\|\mathbf{A}_n\|, \|\mathbf{B}_n\| \leq M < \infty, \quad n = 1, 2, \dots; \quad (342)$$

- 2) $\mathbf{A}_n - \mathbf{B}_n$ converges to zero in the weak norm:

$$\lim_{n \rightarrow \infty} |\mathbf{A}_n - \mathbf{B}_n| = 0, \quad (343)$$

where $|\mathbf{A}| := (\frac{1}{n} \text{tr}[\mathbf{A}^\dagger \mathbf{A}])^{1/2}$.

The key result we use in Section V is then expressed as:

Fact 4. [23, Lemma 4.6] If f is in the Wiener class then $\mathbf{T}_n(f) \sim \mathbf{C}_n(f)$, where the notations \mathbf{T}_n and \mathbf{C}_n are as in (116) and (117).

The following property will be useful later in proving asymptotic equivalence of Toeplitz matrices. The claim about square root matrices follows from [40, Theorem 1] by particularizing the continuous function therein to the square root function, while all other claims are from [23, Theorem 2.1].

Fact 5. Sums and products of asymptotically equivalent matrices are asymptotically equivalent. If the smallest singular values of asymptotically equivalent matrices are uniformly lower bounded, then their inverses are also asymptotically equivalent. Moreover, square roots of asymptotically equivalent positive-semidefinite matrices are asymptotically equivalent.

The relevance of asymptotically equivalent matrices to coding theorems lies in the following fact:

Fact 6. [23, Theorem 2.4] Let \mathbf{A}_n and \mathbf{B}_n be asymptotically equivalent sequences of Hermitian matrices with eigenvalues inside the interval $[m, M]$. Then the eigenvalues of \mathbf{A}_n and \mathbf{B}_n are asymptotically equally distributed on $[m, M]$.

REFERENCES

- [1] I. Csiszár and P. Narayan, “Common randomness and secret key generation with a helper,” *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 344–366, Feb. 2000.
- [2] R. Ahlswede and I. Csiszár, “Common randomness in information theory and cryptography. Part II. CR capacity,” *IEEE Transactions on Information Theory*, vol. 44, no. 1, pp. 225–240, Jan. 1998.
- [3] S. Watanabe and Y. Oohama, “Secret key agreement from vector Gaussian sources by rate limited public communication,” in *Proceedings of 2010 IEEE International Symposium on Information Theory*, pp. 2597–2601.
- [4] H. Weingarten, Y. Steinberg, and S. Shamai, “The capacity region of the Gaussian MIMO broadcast channel,” *IEEE Transactions on Information Theory*, vol. 52, no. 9, pp. 3936–3964, Sept. 2004.
- [5] C. E. Shannon, “Coding theorems for a discrete source with a fidelity criterion,” *IRE National Convention Record*, vol. 4, pp. 142–163, 1959.
- [6] T. M. Cover and J. A. Thomas, *Elements of Information Theory, Second Edition*. John Wiley & Sons, 2012.
- [7] S. Verdú, “On channel capacity per unit cost,” *IEEE Transactions on Information Theory*, vol. 36, no. 5, pp. 1019–1030, May 1990.
- [8] E. Erkip and T. M. Cover, “The efficiency of investment information,” *IEEE Transactions on Information Theory*, vol. 44, no. 3, pp. 1026–1040, Mar. 1998.
- [9] V. Anantharam, A. Gohari, S. Kamath, and C. Nair, “On maximal correlation, hypercontractivity, and the data processing inequality studied by Erkip and Cover,” *arXiv preprint arXiv:1304.6133*, 2013.
- [10] H. S. Witsenhausen, “On sequences of pairs of dependent random variables,” *SIAM Journal on Applied Mathematics*, vol. 28, no. 1, pp. 100–113.

- [11] R. Ahlswede and P. Gács, "Spreading of sets in product spaces and hypercontraction of the Markov operator," *The Annals of Probability*, pp. 925–939, 1976.
- [12] L. Zhao, "Common Randomness, Efficiency, and Actions," *PhD thesis, Department of Electrical Engineering, Stanford University*, 2011.
- [13] J. Liu, P. Cuff, and S. Verdú, "Key capacity with limited one-way communication for product sources," in *Proceedings of 2014 International Symposium on Information Theory*, pp. 1146–1150, Honolulu, Hawaii, June 30–July 4, 2014.
- [14] S. Beigi and A. Gohari, "On the duality of additivity and tensorization," in *Proceedings of 2015 IEEE International Symposium on Information Theory Proceedings (ISIT)*, pp. 2381–2385, Hong Kong, China, June 2015.
- [15] T. A. Courtade, "Outer bounds for multiterminal source coding via a strong data processing inequality," in *Proceedings of 2013 IEEE International Symposium on Information Theory (ISIT)*, pp. 559–563, Istanbul, Turkey, July 2013.
- [16] V. Anantharam, A. A. Gohari, S. Kamath, and C. Nair, "On hypercontractivity and the mutual information between Boolean functions," *The 51st Annual Allerton Conference on Communication, Control, and Computing*, pp. 13–19.
- [17] M. Hayashi, "General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channel," *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1562–1575, Apr. 2006.
- [18] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, Mar. 1993.
- [19] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge University Press, 2011.
- [20] M. Bloch and N. Laneman, "Strong Secrecy from Channel Resolvability," *IEEE Transactions on Information Theory*, vol. 59, no. 12, pp. 8077–8098, Dec. 2013.
- [21] E. C. Song, P. Cuff, and H. V. Poor, "The likelihood encoder for lossy compression," *arXiv:1408.4522v2*.
- [22] R. A. Chou and M. R. Bloch, "Separation of reliability and secrecy in rate-limited secret key generation," *IEEE Transactions on Information Theory*, vol. 60, no. 8, pp. 4941–4957, Aug. 2014.
- [23] R. M. Gray, "Toeplitz and circulant matrices: A review," *Foundations and Trends on Communications and Information Theory*, vol. 2, no. 3, pp. 155–239, 2006.
- [24] P. Cuff, "Distributed channel synthesis," *IEEE Transactions on Information Theory*, vol. 59, no. 11, pp. 7071 – 7096, Nov. 2013.
- [25] Z. Zhang, "Estimating mutual information via Kolmogorov distance," *IEEE Transactions on Information Theory*, vol. 53, no. 9, pp. 3280–3282, Sept. 2007.
- [26] C. E. Shannon, "Certain results in coding theory for noisy channels," *Information and Control*, vol. 1, no. 1, pp. 6–25, 1957.
- [27] A. D. Wyner, "The common information of two dependent random variables," *IEEE Transactions on Information Theory*, vol. 21, no. 2, pp. 163–179, Feb. 1975.
- [28] J. Liu, P. Cuff, and S. Verdú, "Secret Key Generation with One Communicator and a One-Shot Converse via Hypercontractivity," in *Proceedings of 2015 IEEE International Symposium on Information Theory (ISIT)*, pp. 710–714, 2015.
- [29] S. Watanabe, "The rate-distortion function for product of two sources with side-information at decoders," *IEEE Transactions on Information Theory*, vol. 59, pp. 5678–5691, Sept. 2013.
- [30] Y. Liang and G. Kramer, "Rate regions for relay broadcast channels," *IEEE Transactions on Information Theory*, vol. 53, no. 10, pp. 3517–3535, Oct. 2007.
- [31] L. Lovász, "On the Shannon capacity of a graph," *IEEE Transactions on Information Theory*, vol. 25, no. 1, pp. 1–7, 1979.
- [32] N. Alon, "The Shannon capacity of a union," *Combinatorica*, vol. 18, no. 3, pp. 301–310, Mar. 1998.
- [33] T. S. Han and S. Verdú, "Approximation theory of output statistics," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 752–772, Mar. 1993.
- [34] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, Apr. 1993.
- [35] R. A. Horn and C. R. Johnson, *Matrix analysis*. Cambridge University Press, 2012.
- [36] L. Gross, "Logarithmic Sobolev Inequalities," *American Journal of Mathematics*, vol. 97, no. 4, pp. 1061–1083, 1975.
- [37] T. Tao, "Matrix identities as derivatives of determinant identities," [Online]. Available: <http://terrytao.wordpress.com/2013/01/13/matrix-identities-as-derivatives-of-determinant-identities/>.
- [38] H. Weyl, "Über die Gleichverteilung von Zahlen mod. eins," *Mathematische Annalen*, vol. 77, no. 3, pp. 313–352, 1916.
- [39] U. Grenander and G. Szegő, *Toeplitz forms and their applications*. Univ of California Press, 1958.
- [40] J. Gutiérrez-Gutiérrez and P. M. Crespo, "Asymptotically equivalent sequences of matrices and Hermitian block Toeplitz matrices with continuous symbols: Applications to MIMO systems," *IEEE Transactions on Information Theory*, vol. 54, no. 12, pp. 5671–5680, Dec. 2008.

Jingbo Liu received the B.E. degree from Tsinghua University, Beijing, China in 2012 and the M.A. degree from Princeton University, Princeton, NJ, USA in 2014, both in electrical engineering. He is currently pursuing a Ph.D. degree at Princeton University. His research interests include signal processing, information theory, coding theory and the related fields. His undergraduate thesis on a topological viewpoint on non-convex sparse signal recovery received the best undergraduate thesis award at Tsinghua University (2012). He gave a semi-plenary presentation at the 2015 IEEE Int. Symposium on Information Theory, Hong-Kong, China.

Paul Cuff received the B.S. degree in electrical engineering from Brigham Young University, Provo, UT, in 2004 and the M.S. and Ph. D. degrees in electrical engineering from Stanford University in 2006 and 2009. Since 2009 he has been an Assistant Professor of Electrical Engineering at Princeton University.

As a graduate student, Dr. Cuff was awarded the ISIT 2008 Student Paper Award for his work titled Communication Requirements for Generating Correlated Random Variables and was a recipient of the National Defense Science and Engineering Graduate Fellowship and the Numerical Technologies Fellowship. As faculty, he received the NSF Career Award in 2014 and the AFOSR Young Investigator Program Award in 2015.

Sergio Verdú received the Telecommunications Engineering degree from the Universitat Politècnica de Barcelona in 1980, and the Ph.D. degree in Electrical Engineering from the University of Illinois at Urbana-Champaign in 1984. Since 1984 he has been a member of the faculty of Princeton University, where he is the Eugene Higgins Professor of Electrical Engineering, and is a member of the Program in Applied and Computational Mathematics.

Sergio Verdú is the recipient of the 2007 Claude E. Shannon Award, and the 2008 IEEE Richard W. Hamming Medal. He is a member of both the National Academy of Engineering and the National Academy of Sciences.

Verdú is a recipient of several paper awards from the IEEE: the 1992 Donald Fink Paper Award, the 1998 and 2012 Information Theory Paper Awards, an Information Theory Golden Jubilee Paper Award, the 2002 Leonard Abraham Prize Award, the 2006 Joint Communications/Information Theory Paper Award, and the 2009 Stephen O. Rice Prize from the IEEE Communications Society. In 1998, Cambridge University Press published his book *Multuser Detection*, for which he received the 2000 Frederick E. Terman Award from the American Society for Engineering Education. He was awarded a Doctorate Honoris Causa from the Universitat Politècnica de Catalunya in 2005.

Sergio Verdú served as President of the IEEE Information Theory Society in 1997, and on its Board of Governors (1988–1999, 2009–2014). He has also served in various editorial capacities for the *IEEE Transactions on Information Theory*: Associate Editor (Shannon Theory, 1990–1993; Book Reviews, 2002–2006), Guest Editor of the Special Fiftieth Anniversary Commemorative Issue (published by IEEE Press as "Information Theory: Fifty years of discovery"), and member of the Executive Editorial Board (2010–2013). He is the founding Editor-in-Chief of *Foundations and Trends in Communications and Information Theory*. Verdú is co-chair of the 2016 *IEEE International Symposium on Information Theory*, which will take place in his hometown.